Spuren kompromittierter E-Mail-Konten analysieren

Spuren kompromittierter E-Mail-Konten analysieren

Nachdem der erste Teil des Playbooks zu gekaperten E-Mail-Accounts zeigte, wie man die Logs mithilfe von Microsofts zentraler Logfunktion einsammelt, erklärt der zweite Teil, wie man sie auf verdächtige Vorgänge auswertet und welche Rückschlüsse sich daraus ziehen lassen.
Nachdem der erste Teil des Playbooks zu gekaperten E-Mail-Accounts zeigte, wie man die Logs mithilfe von Microsofts zentraler Logfunktion einsammelt, erklärt der zweite Teil, wie man sie auf verdächtige Vorgänge auswertet und welche Rückschlüsse sich daraus ziehen lassen.

- Beim ersten Anzeichen verdächtiger Aktivität rund um E-Mail-Accounts sollte man IT-forensische Untersuchungen anstoßen, um zu verstehen, was genau passiert ist.

Ausgangspunkt der Analyse sind die gesammelten Logdaten und Artefakte.

- Aussagekräftig im Hinblick auf Eindringlinge ins Firmennetz sind unter anderem fehlgeschlagene Anmeldevorgänge, eingerichtete Mailweiterleitungen oder neu vergebene Berechtigungen. Solche Hinweise sollten sorgfältig untersucht werden.
- Die Ursachenforschung und eine Nachbereitung sind das A und O nach der Bewältigung von Sicherheitsvorfällen. Daraus abgeleitete technische Maßnahmen sowie die Sensibilisierung von Mitarbeitenden sollen künftige Angriffe zumindest erschweren.

Die umfassendste Datenquelle zur Analyse von Unregelmäßigkeiten oder Verdachtsmomenten für einen Sicherheitsvorfall bietet Microsofts zentrale Logfunktion Unified Audit Log (UAL). Hier werden Benutzer- und Administratoraktivitäten auch unabhängig vom Einsatz zusätzlicher Produkte wie Microsoft Sentinel oder Microsoft Defender for Identity aufgezeichnet (wie die Logdaten im Detail gesichert werden, beschreibt [1]). Die nachfolgenden Schritte zeigen, wie man bei der Analyse vorgeht und die Logdaten sinnvoll durchsuchen kann.

Schritt 4: Untersuchen der Anmeldeaktivitäten

Jedes Mal, wenn sich ein Benutzer bei seinem Konto anmeldet, wird ein Ereignis im UAL erstellt. Dieses Ereignis enthält wichtige Informationen, etwa die Quell-IP-Adresse, die sich unter anderem für eine geografische Suche verwenden lässt. Die Ergebnisse lassen sich mit den erwarteten geografischen Standorten eines Unternehmens und seiner Nutzer vergleichen. Wenn zum Beispiel ein Unternehmen in Deutschland ansässig ist und keine Niederlassung in Asien hat oder das VPN des Unternehmens nicht zu einer IP-Adresse in Asien auflöst, würde

man keine Ereignisse aus Asien erwarten. Daher wären Anmeldungen aus Asien in diesem Fall verdächtig.

Natürlich kann es auch sein, dass ein Mitarbeiter sich im Urlaub in Asien befindet und sein Firmenhandy dabeihat, dennoch erfordern diese Ausreißer Aufmerksamkeit. Verdächtige Anmeldungen kann man durch die Suche nach bestimmten Schlüsselwörtern im UAL entdecken. Neben der IP-Adresse liefern auch die Uhrzeit sowie Informationen zum verwendeten Gerät (UserAgent: Betriebssystem, Browser et cetera) gute Anhaltspunkte. Ob das verwendete Gerät dem Unternehmen bekannt ist und von der IT verwaltet wird oder nicht, lässt sich ebenfalls den Ereignissen entnehmen. Für die Suche nach verdächtigen Anmeldeereignissen kann man folgende Schlüsselwörter verwenden:

Schlüsselwort	**Bedeutung des Logeintrags**
MailboxLogin	Hinweis auf einen erfolgreichen Log-in-Vorgang
UserLoggedIn	Hinweis auf einen erfolgreichen Log-in-Vorgang
UserLoginFailed	Hinweis auf einen fehlgeschlagenen Log-in-Vorgang
IdsLocked	Hinweis auf einen Brute-Force-Angriff. Der Account wurde gesperrt, da zur viele fehlgeschlagene Anmeldeversuche unternommen wurden.
UserKey=“Not Available“	Hinweis auf einen Brute-Force-Angriff. Die Anmeldung ist fehlgeschlagen, da der Benutzeraccount nicht existiert.

Neben Ereignissen rund um das Log-in können auch Fehlermeldungen zur Multi-Faktor-Authentisierung (MFA) Indikatoren für mögliche schädliche Aktivitäten sein. Ein Angreifer könnte das Passwort eines Anwenders ausgespäht haben, um dann an der MFA-Abfrage zu scheitern. UAL-Einträge mit den folgenden Schlüsselwörtern sollten näher untersucht

werden:

Schlüsselwort	Bedeutung des Logeintrags
UserStrongAuthClientAuthNRequired	Der Benutzer wird zur Bestätigung einer MFA-Abfrage aufgefordert.
UserStrongAuthClientAuthNRequiredInterrupt	fehlgeschlagene MFA-Abfrage

Schritt 5: Untersuchen von Weiterleitungsregeln

Nachdem ein Angreifer einen Benutzeraccount kompromittiert hat, erstellt er häufig Weiterleitungsregeln, um eingehende E-Mails an ein externes Postfach zu schicken. Auf diese Weise kann er die Aktivitäten eines Opfers kontinuierlich überwachen, ohne sich aktiv in das Konto einzuloggen. Selbst wenn das Passwort eines kompromittierten Kontos zurückgesetzt wird, kann der Angreifer weiterhin E-Mails mitlesen.

Ebenfalls beliebt ist der Einsatz von Weiterleitungsregeln zum automatisierten Löschen von E-Mails, um Spuren, die auf Unregelmäßigkeiten hinweisen, zu verwischen. Auch können Weiterleitungsregeln dazu dienen, Spuren vor dem Anwender zu verstecken, indem E-Mails automatisch als gelesen markiert und in einen anderen Ordner (zum Beispiel in den Junk- oder den RSS-Ordner) verschoben werden.

Einem Angreifer bieten sich in einer Microsoft-365-Umgebung gleich mehrere Möglichkeiten, E-Mails an ein externes Postfach umzuleiten. Er kann zunächst einmal Inbox-Regeln anlegen, um E-Mails auszuleiten. Verfügt das Konto zudem über administrative Berechtigungen, ist auch eine Ausleitung über die globalen Postfacheinstellungen oder Exchange-Transportregeln möglich.

Aktive Inbox-Regeln lassen sich mit der Exchange-Management-Shell auffinden, falls sie nicht bereits mittels des im ersten Artikel vorgestellten Tools Hawk extrahiert wurden:

```
Get-InboxRule -Mailbox | ? {$_.forwardto -or $_.forwardasattachmentto -or $_.redirectto}
```

Auch aktive Mailbox-Weiterleitungen kann die Exchange-Management-Shell anzeigen:

```
Get-Mailbox <identity> | Format-List ForwardingSMTPAddress,DeliverToMailboxandForward
```

Der Powershell-Befehl Get-TransportRule liefert eine Übersicht über alle bestehenden Weiterleitungsregeln.

Des Weiteren kann man im UAL potenzielle Angreiferaktivitäten im Zusammenhang mit Weiterleitungsregeln analysieren. Hier lassen sich auch Regeln nachvollziehen, die der Angreifer schon wieder gelöscht hat. Folgende Schlüsselwörter führen zu den relevanten Logeinträgen:

Schlüsselwort	**Bedeutung des Logeintrags**
New-InboxRule	Anlegen einer neuen Weiterleitungsregel (Inbox-Ebene)
New-TransportRule	Anlegen einer neuen Transportregel (Mail Flow Rule)
Set-Mailbox	Änderungen an den Einstellungen einer Mailbox; kann zum Einrichten einer Weiterleitung auf Mailbox-Ebene verwendet werden
Set-InboxRule	Änderung an einer bestehenden Weiterleitungsregel (Inbox-Ebene)
Set-TransportRule	Änderung an einer bestehenden Transportregel (Mail Flow Rule)

Schlüsselwort	Bedeutung des Logeintrags
DeliverToMailboxAndForward	Hinweis darauf, dass eine E-Mail an eine andere Mailbox weitergeleitet wurde
ForwardingSMTPAddress	Hinweis auf eine erfolgte Weiterleitung einer E-Mail
ForwardingAddress	Hinweis auf eine erfolgte Weiterleitung einer E-Mail
SentTo	Hinweis darauf, wohin eine E-Mail gesendet beziehungsweise weitergeleitet wurde
BlindCopyTo	Hinweis darauf, wohin eine E-Mail gesendet beziehungsweise weitergeleitet wurde
ForwardTo	Hinweis darauf, wohin eine E-Mail gesendet beziehungsweise weitergeleitet wurde

Schritt 6: Persistent Access – Hintertüren entdecken

Im nächsten Schritt gilt es zu prüfen, ob der Angreifer Hintertüren eingerichtet hat. Das würde ihm auch im Fall einer Entdeckung noch Zugriff auf die erbeuteten Konten gewähren. Hier gibt es im Wesentlichen drei beliebte Techniken: App-Kennwörter, das Einrichten schädlicher OAuth-Applikationen und die Manipulation von Berechtigungen.

App-Kennwörter dienen eigentlich der Absicherung von Netzwerkprotokollen, die Microsofts „Modern Authentication“ nicht unterstützen. Um die Sicherheit eines Kontos nicht durch die Verwendung des Kennwortes über ein Protokoll, das nicht dem aktuellen Sicherheitsstand entspricht, zu gefährden, bietet Microsoft die Möglichkeit, ein spezifisches Kennwort einzurichten. Es gilt nur für dieses Protokoll.

Wird es kompromittiert, erhält der Angreifer nur Zugriff zu einem einzelnen Protokoll, zum Beispiel IMAP oder POP, nicht aber zum gesamten Nutzerkonto. Doch Angreifer können diese Funktion auch missbrauchen, damit sie über ein selbst eingerichtetes App-Kennwort auch nach Änderung des Kennworts im Azure AD noch Zugriff auf die Mails eines Nutzers haben und gegebenenfalls auch weiterhin illegitime Mails verschicken können.

Zur Prüfung auf App-Passwörter sollten Administratoren zum einen im Azure AD die für den jeweiligen Benutzeraccount hinterlegten Authentifizierungsmethoden sichten und zum anderen im Kontext des Kontos selbst die Liste der App-Kennwörter abrufen (siehe ix.de/z2y8).

Anwendungen als Hintertür missbrauchen

Auch Enterprise-Applikationen, die sich mittels OAuth authentifizieren, können als Hintertür zu einem kompromittierten Konto genutzt werden. Berechtigt der Angreifer eine von ihm kontrollierte Enterprise-Applikation zum Zugriff auf das übernommene Konto, erlaubt er damit der Applikation, Aktionen im Kontext des Benutzers durchzuführen.

So ist über diese Applikation auch nach Änderung des Kennworts ein Zugriff mit den gewährten Berechtigungen möglich. Um zu prüfen, ob im Rahmen eines Angriffs Enterprise-Applikationen Berechtigungen erhielten – Microsoft spricht in diesem Zusammenhang von „Illicit Consent Attacks“ –, gibt es mehrere Möglichkeiten.

Administratoren können die Berechtigungen über das Azure-Active-Directory-Portal über den Menüpunkt „Nutzer“ und Auswahl des betroffenen Nutzerkontos prüfen. Eine globale Liste zeigt im Azure AD der Unterpunkt Enterprise-Applikationen. Wer lieber mit PowerShell arbeitet, kann das Skript AzureADPSPermissions.ps1 (siehe ix.de/z2y8) verwenden, um sämtliche OAuth-Berechtigungen eines Tenant in eine CSV-

Datei zu exportieren und anschließend zu überprüfen.

Das Hinzufügen von Enterprise-Applikationen beziehungsweise das Erteilen von Berechtigungen für sie im Analysezeitraum wird im UAL erfasst. Das Werkzeug Hawk extrahiert die Artefakte automatisch (Azure_Application_Audit.csv und Consent_Grant.csv).

Eine Variante zum Phishing mittels OAuth-Applikationen ist das sogenannte Device-Code-Phishing, mit dem sich Office-365-Konten übernehmen lassen. Details zu dieser Angriffstechnik sowie Hinweise zur Detektion und Aufklärung finden sich in einem Artikel des Sicherheitsforschers Nestori Syynimaa (siehe ix.de/z2y8).

Schlüsselwort	Bedeutung des Logeintrags
Add 0Auth2PermissionGrant	Einer Enterprise-Applikation wurden Berechtigungen erteilt.
Consent to application	Einer Enterprise-Applikation wurden Berechtigungen durch einen Admin erteilt.
Add app role Assignment grant to use	Ein Benutzer wurde einer Applikation hinzugefügt.

Hat ein Angreifer mehrere Konten eines Unternehmens kompromittiert, kann er sie dazu missbrauchen, Hintertüren einzurichten, indem er den anderen kompromittierten Konten Zugriff auf eine Mailbox gibt. Solange die Verteidiger nicht sämtliche betroffenen Konten identifizieren, behält der Angreifer weiter Zugriff.

Ereignisse im Zusammenhang mit Berechtigungsänderungen lassen sich durch die Suche nach den folgenden Schlüsselwörtern im UAL ausfindig machen:

Schlüsselwort	Bedeutung des Logeintrags
Add-MailboxPermission	Neue Berechtigungen auf ein Postfach wurden vergeben.

Schlüsselwort	Bedeutung des Logeintrags
Add-MailboxFolderPermission	Neue Berechtigungen auf einen Order in einem Postfach wurden vergeben.
Add-RecipientPermission	Hinweis darauf, dass einem Benutzer die „Senden als“-Berechtigung zugewiesen wurde.
Set-MailboxFolderPermission	Bestehende Berechtigungen eines Ordners in einem Postfach wurden geändert.

Hat ein Angreifer sogar ein Konto mit administrativen Berechtigungen gekapert, kann er zudem eigene neue Benutzerkonten anlegen, die dann als Hintertür dienen. Auch das hinterlässt Spuren im UAL.

Schlüsselwort	Bedeutung des Logeintrags
Added user	Ein neuer Benutzer wurde angelegt.

Schritt 7: Datenexfiltration analysieren

Bestätigt es sich, dass jemand Unbefugtes Zugriff auf das Unternehmensnetzwerk hatte, stellt sich in erster Linie die Kernfrage: Worauf hat der Angreifer zugegriffen? Dem zugrunde liegt oft die (späte) Erkenntnis über Art und Umfang der Informationen, die mit einem Benutzerkonto prinzipiell erreichbar wären, verbunden mit dem Wunsch, dieses Worst-Case-Szenario irgendwie einzugrenzen.

Hier zunächst die schlechte Nachricht vorweg: Es ist in der Praxis selten möglich, einen Negativbeweis zu führen, also festzustellen, was die Angreifer nicht mitgenommen haben. Die Aussagekraft der Artefakte ist meist begrenzt, da schlicht nicht alles protokolliert wird. In der Regel muss bei einer gesicherten Kompromittierung eines Kontos unterstellt werden, dass der Angreifer alle erreichbaren Inhalte ausgespäht hat. Das hat erhebliche Konsequenzen beispielsweise für die

datenschutzrechtliche Bewertung eines Vorfalls.

Die gute Nachricht ist, dass auch Microsoft das erkannt hat. Konten, die mit einer E5-Lizenz ausgestattet sind, verfügen über eine „erweiterte Überwachung“. Diese Funktion protokolliert unter anderem Zugriffe auf einzelne E-Mails, was die Chance auf den seltenen Negativbeweis zumindest für die Inhalte des Postfachs deutlich verbessert.

Im UAL finden sich dann Einträge der Art MailItemsAccessed. Diese haben unter anderem ein Attribut MailAccessType, das zwischen Bind und Sync unterscheidet.

Operation	Bedeutung des Logeintrags
MailItemsAccessed	Hinweis auf den erfolgten Zugriff auf Inhalte eines Postfachs

Bind-Einträge werden erzeugt, wenn eine einzelne E-Mail abgerufen wird. Die ID der Nachricht steht dann im Attribut InternetMessageId. Die Protokollierung unterliegt jedoch einer wichtigen Einschränkung: Werden innerhalb von 24 Stunden mehr als 1000 Zugriffe dokumentiert, wird die Protokollierung für Bind-Ereignisse für 24 Stunden ausgesetzt (Throttle).

Zuerst sollte also geprüft werden, ob das UAL Einträge des Typs MailItemsAccessed für die zu untersuchende Mailbox enthält. Anschließend gilt es auszuschließen, dass ein Throttling stattgefunden hat. Dazu schaut man, ob es bei den MailItemsAccessed-Ereignissen welche gibt, die beim Attribut IsThrottled den Wert True vermerkt haben. Im Idealfall gibt es keinen solchen Eintrag.

Welche Sitzung gehört zu wem?

Der nächste Schritt besteht darin, die zum Angreifer gehörenden Sitzungen zu ermitteln. Dafür gleicht man die MailItemsAccessed-Vorgänge im UAL mit den Informationen des Angreifers (verdächtige Log-in-Aktivitäten, IP-Adressen, Zeitstempel, Art des Zugriffs) und den Informationen über den

legitimen Anwender ab. Die Einträge haben mitunter mehrere Session-IDs und IP-Adressen für ein Benutzerkonto. Anhand der in den vorangegangenen Schritten ermittelten Kompromittierungsindikatoren lässt sich feststellen, welche Sitzungen wahrscheinlich legitim oder gültig sind. Einige Sitzungen haben möglicherweise keine Session-ID, weil für die Anmeldung eine alte (Legacy-)Authentifizierung verwendet wurde. Die verdächtigen MailItemsAccessed-Einträge werden dann weiter analysiert.

Sync-Einträge entstehen immer dann, wenn ein E-Mail-Client, beispielsweise Outlook, ein Postfach synchronisiert und dabei Inhalte auf einen lokalen Computer herunterlädt. Hierbei entsteht kein Logeintrag pro Element, sondern pro Ordner des Postfachs. Finden sich im UAL MailItemsAccessed-Einträge mit dem MailAccessType Sync, die dem Angreifer zugeordnet werden, so muss man davon ausgehen, dass alle E-Mails im synchronisierten Ordner kompromittiert wurden.

Zuletzt bleiben die Bind-Vorgänge, die dem Angreifer zugeordnet werden. Diese enthalten eine InternetMessageID. Um damit auf die eigentlichen Nachrichten schließen zu können, ist es notwendig, das Message Trace Log mit den IDs abzugleichen. Leider reicht das Message Trace Log nicht so weit zurück wie die Einträge im UAL, sondern lediglich zehn Tage. Auch lässt sich die InternetMessageID nicht als Suchparameter im Rahmen einer Suche nach Beweismitteln (E-Discovery) verwenden.

Können E-Mails nicht mehr über das Message Trace Log zugeordnet werden, bleibt lediglich der Weg, das Postfach selbst zu exportieren und die E-Mails zu durchsuchen. Die ID ist in den Eigenschaften der E-Mails gespeichert. Der Export des Postfachs lässt sich außerdem über die E-Discovery-Funktion realisieren, die auch bereits gelöschte Elemente berücksichtigt (sofern entsprechende Aufbewahrungsrichtlinien konfiguriert sind und die Elemente noch vorgehalten werden).

Rekonstruieren, was geklaut wurde

Wie beschrieben können E-Mails auch über Weiterleitungsregeln abgegriffen werden. Findet man bei einer Untersuchung solche Regeln, kann sowohl das UAL (siehe Schritt 5) wie auch die Logik der Regeln selbst Aufschluss über die betroffenen Inhalte geben. Neben dem Abgleich der Einträge im UAL mit dem Message Trace Log sollte die Mailbox nach den Parametern der Regel(n) durchsucht werden.

Sofern ein Angreifer Zugang zu einem Konto mit administrativen Berechtigungen und der E-Discovery-Suche hatte, kann er auch auf diesem Weg Inhalte gesucht und exportiert haben. Hinweise darauf lassen sich wieder im UAL finden.

Analog zu den E-Mails sind alle weiteren Inhalte zu berücksichtigen, die mit dem kompromittierten Konto für den Angreifer erreichbar waren. Das beinhaltet sowohl in OneDrive geteilte Dateien wie Teams-Nachrichten und SharePoint-Seiten als auch sämtliche nachgelagerten Applikationen, die Azure AD zur Authentifizierung verwenden. Die Analyse ist allerdings oft sehr individuell und würde den Rahmen dieses Artikels sprengen.

Schritt 8: Remediation

Nachdem die Aktivitäten eines Angreifers nachvollzogen wurden, gilt es, alles rückgängig zu machen, also alle gefundenen Weiterleitungsregeln, Enterprise-Applikationen, App-Kennwörter et cetera zu entfernen und die Kennwörter der betroffenen Konten, falls noch nicht geschehen, zurückzusetzen. Auch sollten alle Analysen und eingeleiteten Maßnahmen dokumentiert und mit den zugehörigen Logdateien aufbewahrt werden.

Zeigte die Untersuchung einen unberechtigten Zugriff auf Postfächer, handelt es sich um einen meldepflichtigen Vorfall gemäß der DSGVO. Dementsprechend ist eine Erklärung an den zuständigen Landesdatenschutzbeauftragten verpflichtend. Dabei

gilt es, die gesetzlichen Fristen zu beachten. Binnen 72 Stunden ab dem Zeitpunkt der Kenntnisnahme muss die Meldung erfolgen. Zu diesem Zeitpunkt ist gegebenenfalls noch nicht das gesamte Ausmaß des Vorfalls bekannt. In diesem Fall sollte die Meldung einfach alle bisher gesicherten Informationen enthalten. Die Meldung sollte durch den benannten Datenschutzbeauftragten des betroffenen Unternehmens erfolgen.

Neben den Datenschutzbehörden müssen gegebenenfalls auch die betroffenen Personen informiert werden. Dies ist dann der Fall, wenn besonders heikle personenbezogene Daten gemäß Art 9 DSGVO – also beispielsweise religiöse oder weltanschauliche Überzeugungen oder Gesundheitsdaten – betroffen sind. In diesem Fall sind die betroffenen Personen direkt zu benachrichtigen. Die Prüfung einer solchen Meldepflicht obliegt dem Datenschutzbeauftragten. Gegebenenfalls sollte bei Verdacht auf einen solchen Fall juristischer Beistand hinzugezogen werden.

Schritt 9: Root Cause Analysis – woran liegts?

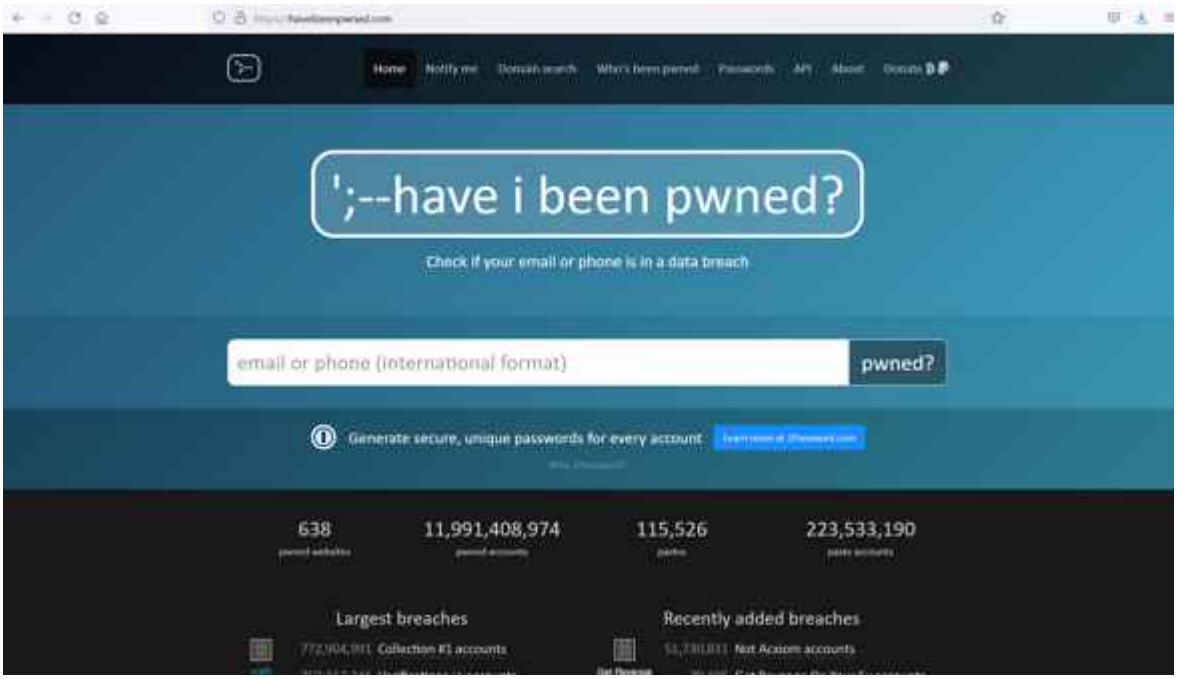
Nachdem aufgeklärt ist, wie ein Angreifer vorgegangen ist und was er genau getan hat, bleibt noch die Frage, wie das passieren konnte. Wie hat er initial Zugang erhalten?

Auch hier ist leider keine pauschale Anleitung möglich, doch die häufigsten Ursachen sind folgende:

- Password Spraying / Brute Force / einfach zu erratende Passwörter: Allen drei Szenarien ist gemeinsam, dass sie in der Regel mit mehrfachem Ausprobieren einhergehen. In den Logs äußert sich dies durch multiple fehlgeschlagene Log-in-Versuche bei einem oder mehreren Konten, ausgehend von derselben IP-Adresse und/oder ähnlichen Parametern wie User-Agent, Protokoll und Zeitpunkt.
- (Spear-)Phishing: Bei einem Phishingangriff erhält das

Opfer eine E-Mail, die einen Link oder einen Anhang enthält, über den die Zugangsdaten abgegriffen werden (funktioniert teilweise auch bei MFA) oder eine Enterprise App via OAuth-Berechtigungsanfrage untergeschoben wird. In dem Fall sind keine gehäuften fehlgeschlagenen Log-in-Versuche zu beobachten. Stattdessen gilt es, die Phishingmail im Postfach oder den aufgerufenen Link ausfindig zu machen.

- Password Re-use / Leaked Credentials: Oft verwenden Anwender ein Passwort für mehrere Dienste und Konten oder recyceln ein privates Passwort für Firmenzwecke. In dem Fall kann es sein, dass das Kennwort bei einem der anderen Dienste ausgespäht wurde und dann für die Anmeldung am Microsoft-365-Account ausprobiert wird. Auch hier ist nicht unbedingt eine gehäufte Anzahl an Fehlversuchen zu beobachten, sofern nicht zusätzlich MFA aktiviert ist. Um der Ursache in dem Fall näherzukommen, empfiehlt es sich, mit dem Benutzer ein offenes Gespräch zu führen oder die Unternehmens-E-Mail des Anwenders bei seriösen Diensten wie haveibeenpwned.com einzugeben (siehe Abbildung).



Ob ein Passwort geleakt wurde, kann man beispielsweise bei Diensten wie „Have I Been Pwned“ herausfinden. Dieser Dienst

des australischen Sicherheitsforschers Troy Hunt hat einen guten Ruf, da er nicht das Passwort selbst, sondern nur den Benutzernamen abfragt.
Nach der erfolgreichen Bewältigung des potenziellen oder realen Sicherheitsvorfalls sollte immer auch geprüft werden, welche Lektionen man daraus lernen kann und welche Maßnahmen zu ergreifen sind, damit ähnliche Vorfälle in Zukunft seltener oder gar nicht mehr vorkommen. Dabei soll es explizit keine Schuldzuweisungen geben, das Stichwort lautet hier vielmehr „Blameless Post Mortem“.

Awareness-Maßnahmen und Schulungen können gängige Betrugsmuster vermitteln und damit die Anfälligkeit der Mitarbeitenden für solche Angriffe verringern. Klar definierte Prozesse zur Veranlassung von Zahlungen helfen außerdem, bestimmte Arten von finanziellem Betrug zu erschweren. Häufig werden aber im Rahmen der Vorfallsbehandlung vor allem technische Gegebenheiten identifiziert, die die Kompromittierung erleichtert oder die Untersuchung des Vorfalls erschwert haben. So ist es hilfreich, die SPF-, DKIM- oder DMARC-Konfiguration (Sender Policy Framework; DomainKeys Identified Mail; Domain-based Message Authentication, Reporting and Conformance) nachzurüsten, falls sie im Vorfeld des Vorfalls noch nicht aktiv war, die Protokollierung lässt sich verbessern, wenn Logs für die Aufklärung des Angriffs fehlten, oder das Installieren von OAuth-Anwendungen kann für Nutzer des Tenants eingeschränkt werden, falls Angreifer solche Anwendungen als Hintertür installiert haben.

Microsoft gibt im Rahmen einer Referenzarchitektur zahlreiche Hinweise für das Absichern von Microsft-365- und Azure-AD-Umgebungen (siehe ix.de/z2y8), die im Nachgang eines Vorfalls (re-)evaluiert werden und bei Bedarf in das Sicherheitskonzept des Unternehmens integriert werden können. Dedizierte Dienste wie Microsoft Defender for Office, Microsoft Defender for Identity oder Microsoft Defender for Cloud Apps können gegen Angriffe schützen oder bei ihrer Entdeckung und Aufbereitung helfen. Allerdings sind sie häufig nur in den teureren

Lizenzen der Microsoft-Produkte enthalten oder müssen sogar separat lizenziert werden. (ur@ix.de)

1. Quellen
2. Jens Lüttgens, Dominik Oepen; E-Mail-Betrug in MS-365-Umgebungen; iX 12/2022, S. 102
3. Vertiefende Microsoft-Artikel, das erwähnte PowerShell-Skript sowie die Microsoft-Referenzarchitektur sind über ix.de/z2y8 zu finden.

Introducing a new phishing technique for compromising Office 365 accounts

The ongoing global phishing campaings againts Microsoft 365 have used various phishing techniques.
Currently attackers are utilising forged login sites and OAuth app consents. In this blog, I'll introduce a new phishing technique based on Azure AD device code authentication flow.
I'll also provide…

Betrüger bestehlen sich gegenseitig

Sicherheitsexperten von Sophos analysierten drei Untergrundforen und deren Schlichtungsräume für Streitigkeiten. Fazit: Wenn zwei Kriminelle sich streiten, freut sich die Verteidigung, die dadurch wertvolle Informationen erhält.

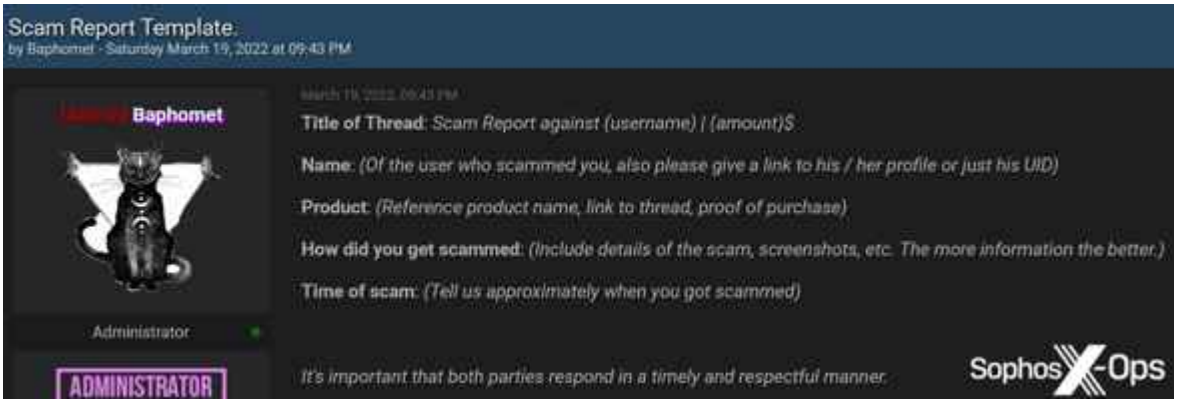
Markt + Trends | IT-Sicherheit

Dass die Schattenwelt der Internetkriminellen genauso arbeitsteilig agiert wie die „richtige“ Wirtschaft, ist seit einigen Jahren bekannt. Sicherheitsforscher von Sophos X-Ops veröffentlichen nun im ersten Teil einer vierteiligen Serie neue Details (siehe ix.de/zey7). So verfügen die untersuchten Untergrundforen Exploit und XSS, zwei russischsprachige Cybercrime-Foren für Access as a Service (AaaS), und die englischsprachige, auf Datenlecks spezialisierte Plattform BreachForums mit Marktplatzfunktion über spezielle Schlichtungsräume zur Beilegung von Streitigkeiten. Dort können Nutzer Betrug, Angriffe und Abzocker melden.

Die „Betrüger betrügen Betrüger“-Masche scheint lukrativ zu sein: In einem Zeitraum von zwölf Monaten analysierte Sophos X-Ops rund 600 Betrugsfälle, bei denen die Bedrohungsakteure

allein in diesen drei Foren mehr als 2,5 Millionen US-Dollar aneinander verloren.

Geld ist den Forschern von Sophos zufolge nicht die einzige Motivation, die die Kriminellen gegeneinander agieren lässt. Auch persönliche Streitigkeiten, Rivalitäten zwischen den Akteuren oder auch der Wunsch, den Ruf des anderen zu beschädigen oder den eigenen zu verbessern, gehören zu den Ursachen.



Im Untergrund wie im echten Leben: Beschwerde führen per Formular. *Sophos*

Die Angriffe gingen über das übliche „Abzocken und Verschwinden“ hinaus. Die Forscher sahen Empfehlungsbetrügereien, vorgetäuschte Datenabflüsse und gefälschte Tools, Phishing, URL-Hijacking, „alt rep“-Betrug (das Verfälschen von Reputationswerten durch Einsatz von „Sockpuppets“, also Fake-Accounts), falsche Bürgen, Erpressung, nachgemachte Konten und Backdoors. Auch konnten die Forscher Fälle beobachten, in denen sich betrogene Bedrohungsakteure wiederum an ihren Betrügern rächten.

Die Sicherheitsforscher fanden überdies Indizien für langfristigen, groß angelegten Betrug in Form von neunzehn Websites, alle von derselben Person oder Gruppierung erstellt, die kriminellen Marktplätzen täuschend ähnlich sehen. Sie fordern von neuen Nutzern eine Aktivierungsgebühr in Höhe von 100 Dollar.

Verteidiger

Theoretisch könnte es der Allgemeinheit völlig gleichgültig sein, wie Kriminelle und Betrüger zueinander stehen oder miteinander umgehen. Aber, erläutert Matt Wixey, Senior Threat Researcher bei Sophos, „da Kriminelle oft viele Beweise vorlegen müssen, wenn sie über die Betrügereien berichten, denen sie selbst zum Opfer gefallen sind, liefern sie eine Fülle von taktischen und strategischen Informationen über ihre Operationen – eine bisher ungenutzte Ressource“. Diese Schlichtungsberichte vermittelten außerdem einen Einblick in die Prioritäten der Angreifer, ihre Rivalitäten und Allianzen, „und, ironischerweise, wie anfällig sie für die gleichen Arten von Täuschung sind, die sie gegen ihre Opfer einsetzen“, so Wixey. (ur@ix.de)

ix.de/zey7

- **The scammers who scam scammers on cybercrime forums: Part 1**
- **Folien des Black-Hat-Vortrags von Sophos**
- **BMI-Papier: Strategie zur Bekämpfung der Schweren und Organisierten Kriminalität**
- **NSA-Empfehlungen für Entwickler zum Absichern der Supply Chain**
- **Projekt Sigstore – Software Signing for Everybody**
- **Konzept von Sigstore**
- **verinice.veo DSMS**
- **Playlist der Vorträge der Black Hat 2022**
- **Aagon Bitlocker-Management**

The scammers who scam scammers on

cybercrime forums: Part 1

A shadowy sub-economy is more than just a curiosity – it's booming business, and also an opportunity for defenders. In the first of a four-part series, we look at the forums involved, and how they …

Die Betrüger, die Betrüger in Cybercrime-Foren betrügen: Teil 1

Eine Schattenwirtschaft ist mehr als nur eine Kuriosität – sie ist ein boomendes Geschäft und auch eine Chance für Verteidiger. Im ersten einer vierteiligen Serie betrachten wir die beteiligten Foren und wie sie mit Betrügern umgehen, die Betrüger betrügen

Geschrieben von Matt Wixey

07. Dezember 2022

Bedrohungsforschung AaaS BreachForums Exploit RaidForums Marktplätze empfohlene Betrug Sophos X-Ops XSS

Auf kriminellen Marktplätzen lauert an jeder Ecke ein Betrug. Bereits 2009 wies Microsoft darauf hin, dass die Untergrundwirtschaft voller Unehrlichkeit sei, und 2017 berichtete Digital Shadows über eine Datenbank von „Rippern" (Betrüger, die Kriminelle betrügen), die von Marktplatzbenutzern erstellt wurde. In unserer jüngsten Berichterstattung über Genesis Market haben wir mindestens eine betrügerische Imitation von Genesis festgestellt, die darauf abzielt, naive Möchtegern-Cyberkriminelle (und möglicherweise unerfahrene Sicherheitsforscher und Journalisten) von ihrem Geld zu trennen.

Aber im Allgemeinen hat das Thema nicht viel Aufmerksamkeit erhalten. Warum sollte es denn auch? Wenn Betrüger Kriminelle ins Visier nehmen, umso besser, oder? Zumindest greifen sie sich gegenseitig an, nicht Organisationen oder die breite Öffentlichkeit.

Wir dachten, dass da noch mehr dahintersteckt, also verbrachten wir ein paar Wochen damit, Betrüger zu untersuchen, die Betrüger in drei prominenten Cybercrime-Foren betrügen – eine Recherche, die unserer Meinung nach noch nie zuvor durchgeführt wurde. Und wir fanden fünf überraschende Dinge.

1. Es ist ein großes Geschäft – eine Subökonomie für sich. In den letzten 12 Monaten haben Cyberkriminelle allein in diesen drei Foren über 2,5 Millionen US-Dollar durch Betrug verloren. Tatsächlich ist es ein so lange bestehendes und prominentes Problem, dass Forenadministratoren spezielle „Schlichtungsräume“ eingerichtet haben, in denen Benutzer Betrug, Angriffe und Ripper melden können.

2. Geld ist nicht das einzige Motiv, und es sind nicht nur niederrangige Bedrohungsakteure beteiligt. Persönliche Probleme, Rivalitäten und der Wunsch, den Ruf zu zerstören (oder manchmal zu verbessern), können alle zu Betrug führen. Und es sind nicht nur kleine Gauner. Wir sahen prominente Bedrohungsakteure, die entweder des Betrugs beschuldigt wurden oder selbst Opfer von Betrug wurden.

3. Die Angriffe gehen über das übliche „Rip-and-Run“ hinaus. Wir sahen Verweis-Nachteile, gefälschte Datenlecks und Tools, Typosquatting, Phishing, „Alt-Rep“-Betrug (die Verwendung von Sockenpuppen, um die Reputationswerte künstlich aufzublähen), gefälschte Bürgen, Erpressung, imitierte Konten und Backdoor-Malware. Wir haben sogar Fälle gefunden, in denen sich Bedrohungsakteure rächen, indem sie die Betrüger betrügen, die sie betrogen haben.

4. Wir haben Beispiele für langfristigen, groß angelegten Betrug gefunden. Eine der größten Überraschungen kam, als wir uns mit dieser nachgeahmten Genesis-Seite befassten. Mit einiger Detektivarbeit entdeckten wir neunzehn weitere Websites, die alle von derselben Person oder Gruppe erstellt wurden, alle kriminelle Marktplätze imitierten und alle darauf abzielten, Benutzer dazu zu verleiten, eine „Aktivierungsgebühr“ von über 100 US-Dollar zu zahlen. Wir wissen nicht genau, wer hinter all diesen Seiten steckt, aber wir haben versuchsweise Links zu einem Drogenhändler entdeckt, der auf mehreren dunklen Websites operiert.

So weit, so *Schadenfreude* – aber die große Frage ist immer noch: wen interessiert das? Warum spielt es eine Rolle, wenn sich Kriminelle gegenseitig angreifen? Hier wird es wirklich faszinierend.

5. Betrugsberichte sind eine reichhaltige und wenig erforschte Informationsquelle. Bedrohungsakteure sind sich bewusst, dass kriminelle Foren überwacht werden, und setzen daher häufig auf gute Betriebssicherheit. Wenn sie selbst Opfer von Verbrechen sind – nun ja, nicht so sehr. Da Forenregeln Beweise für Betrugsvorwürfe verlangen, posten Angreifer, denen Unrecht getan wurde, oft gerne Screenshots von privaten Gesprächen und Quellcode, Identifikatoren, Transaktionen, Chatprotokollen und detaillierte Berichte über Verhandlungen, Verkäufe und Fehlerbehebung.

Diese versteckte Subwirtschaft ist nicht nur eine Kuriosität. Es gibt uns Einblicke in die Forumskultur; wie Bedrohungsakteure kaufen und verkaufen; ihre taktischen und strategischen Prioritäten; ihre Rivalen und Allianzen; ihre Anfälligkeit für Täuschung – und spezifische, diskrete Informationen über sie.

In den nächsten Wochen werden wir die Ergebnisse unserer ausführlichen Untersuchung zu diesem Thema teilen – beginnend mit einem Überblick über die beteiligten Foren, wie sie mit

Betrug umgehen, wer wen betrügt und die Größe der Subwirtschaft.

Sie können sich auch unseren Black-Hat-Vortrag zu dieser Forschung ansehen.

Willkommen im Dschungel

Um unsere Untersuchung einzuleiten, haben wir Betrügereien in zwei der ältesten und bekanntesten russischsprachigen Cybercrime-Foren, Exploit und XSS, untersucht. Wir haben auch Betrügereien von BreachForums, dem Nachfolger von RaidForums, das im April 2022 gestartet wurde, aufgenommen.

Die Foren

Exploit ist relativ exklusiv und ein beliebter Marktplatz für Access-as-a-Service (AaaS)-Angebote , bei denen Initial Access Brokers (IABs) den Zugang zu kompromittierten Netzwerken verkaufen . Aber Bedrohungsakteure kaufen und verkaufen dort auch viele andere illegale Inhalte – Malware, Datenlecks, Infostealer-Protokolle, Anmeldeinformationen und mehr. In der Vergangenheit besuchten Ransomware-Gruppen und -Partner Exploit, obwohl dies nach dem Angriff auf die Colonial Pipeline im Jahr 2021 verdeckter wurde, als sowohl Exploit als auch XSS Ransomware-Diskussionen öffentlich untersagten, um negative Aufmerksamkeit zu vermeiden . Heutzutage wird die Rekrutierung von Ransomware-Affiliates in beiden Foren fortgesetzt, obwohl dies eher unter dem Deckmantel von Euphemismen wie „Pentester“ erfolgt.

XSS, früher bekannt als DaMaGeLaBs, ist ebenfalls gut etabliert, obwohl die Mitgliedschaft weniger exklusiv ist als Exploit. Es hostet auch viele AaaS-Angebote und verschiedene andere Inhalte.

Schließlich ist BreachForums der Nachfolger von RaidForums, einem Marktplatz, der sieben Jahre lang lief, bevor er Anfang

2022 von den Strafverfolgungsbehörden beschlagnahmt wurde . BreachForums ist wie RaidForums ein englischsprachiges Cybercrime-Forum und ein Marktplatz, der sich auf Datenlecks spezialisiert hat, darunter personenbezogene Daten, Kreditkarten, Anmeldeinformationen und Ausweisdokumente.

Alle drei Seiten haben dedizierte Schlichtungsräume – Exploit (mit ungefähr 2500 gemeldeten Betrügereien) und XSS (mit ungefähr 760) haben sie seit Mitte der 2000er Jahre und BreachForums seit ihrer Gründung im April 2022. Andere kriminelle Marktplätze, wie Verified, haben sie Sie auch.

Tatsächlich hat Exploit zwei Räume – einen für offene Ansprüche und einen anderen, der als „Schwarze Liste“ bezeichnet wird und bestätigte Betrugsfälle dokumentiert.

Abbildung 1: Arbitration-Bereich von Exploit

Zusätzlich zu einem speziellen Schlichtungsraum führt XSS auch eine lange „Ripper-Liste“, einen Index von Betrugsseiten.

Abbildung 2: Die Ripper-Liste von XSS

Eine Übersicht über Betrugsstatistiken

Wir haben uns alle Betrugsberichte der letzten 12 Monate angesehen, in denen Geldbeträge angegeben wurden. (Mit BreachForums gingen wir zurück zum ersten aufgezeichneten Betrug, da das Forum noch nicht so lange existiert.)

	Exploit (offene Ansprüche)	**Exploit („Schwarze Liste“)**	**XSS**	**Verletzungsforen**
Ansprüche	211	236	120	21
Gesamtmenge	$1,021,998	$863,324	$509,901	$143,722
Bedeuten	$4,843.54	$3,658	$4,249.18	$6,843.90

Modus	$1000	$500	$150	$500
Median	$600	$500	$500	$200
Bereich	$15 – $160,000	$5 – $150,000	$10 – $160,000	$2 – $134,000

Tabelle 1: Eine Zusammenfassung von 12 Monaten Betrugsmeldungen (alle Beträge in USD)

Dies ist zwar nur eine Momentaufnahme, gibt uns aber einige nützliche Einblicke. Erstens beträgt der durch Betrug verlorene Gesamtbetrag (und denken Sie daran, dass dies nur Betrugsberichte betrifft, in denen bestimmte Beträge erwähnt werden – manche tun dies nicht) 2.538.945 $. Das ist eine beträchtliche Menge, wenn man bedenkt, dass es sich nur um drei Foren handelt.

Zweitens ist Exploit das Schlimmste für Betrug, sowohl in Bezug auf die Anzahl der Berichte als auch auf das Geld, das Betrügern verloren geht. Es hat etwa doppelt so viele Mitglieder wie XSS und kann aufgrund seines guten Rufs auch mehr Betrüger anziehen.

Drittens ist der durchschnittliche als gestohlen gemeldete Betrag in allen drei Foren ähnlich, ebenso wie die Bandbreite – was darauf hindeutet, dass das Ausmaß der Betrügereien unabhängig vom Forum gleich ist.

Opfer haben Betrugsmeldungen für nur 2 US-Dollar eingereicht; Angreifer scheinen genauso empört über den Diebstahl ihres Geldes zu sein wie alle anderen, egal wie hoch der Betrag ist.

Am oberen Ende gehen die Betrügereien auf allen drei Marktplätzen in den sechsstelligen Bereich, obwohl dies die Ausnahmen sind. Viele Betrügereien bringen relativ unbedeutende Beträge ein.

Abbildung 3: Niedrige Schadensummen im XSS-Schlichtungsraum

Abbildung 4: Niedrige Forderungsbeträge im Schlichtungsraum von BreachForums

Abbildung 5: Ein Beispiel für einen größeren Betrugsanspruch auf Exploit (130.000 $). Beachten Sie die vielen Details in diesem Betrugsfall, der Informationen über Verhandlungen und Projekte enthält

Bevor wir uns mit dem Schlichtungsverfahren befassen, lohnt es sich zu untersuchen, warum Betrug so weit verbreitet ist. Bereits 2009 argumentierte Microsoft, dass die illegale Cyberkriminalität keine „kriminelle Utopie des leichten Geldes“ sei, sondern ein „Zitronenmarkt“, auf dem die Anwesenheit von Rippern effektiv eine Steuer auf jede Transaktion einführte.

Auch wenn sich die Zeiten geändert haben und Cyberkriminalität immer mehr zur Ware geworden ist, sind kriminelle Marktplätze immer noch der perfekte Nährboden für Betrüger und Ripper. Es gibt keinen Rückgriff auf die Strafverfolgung; es ist eine (halb) anonyme Kultur, die Privatsphäre betont; Websites sind so exklusiv, dass zumindest ein gewisses Maß an implizitem Vertrauen besteht; Sie werden von Kriminellen bevölkert, die sich wohl kaum als potenzielle Opfer betrachten und daher möglicherweise weniger auf der Hut vor Betrug sind. es ist ein offener Markt ohne Regulierung oder Qualitätssicherung; Transaktionen werden mit Kryptowährungen durchgeführt, die effektiv unauffindbar gemacht werden können; und Sicherheitsvorkehrungen wie Bürgen sind optional (und können, wie wir im nächsten Teil unserer Serie sehen werden, selbst in den Dienst von Betrügereien gestellt werden).

Was unternehmen kriminelle Marktplätze

gegen Betrug?

Die Administratoren krimineller Foren sind sich bewusst, dass Betrug ein Problem darstellt. Zusätzlich zu den Schlichtungsstellen verfügen die meisten Marktplätze über sichtbare Warnungen vor Betrügern und befürworten die Verwendung von Bürgen (manchmal auch als „Zwischenhändler“ oder „Mittelsmänner“ bezeichnet) während des Verkaufs – eine Form der Treuhand.

Abbildung 6: Eine Warnung vor Betrug auf der Titelseite von BreachForums

Andere Foren gehen weiter. Verified zum Beispiel warnt Benutzer ausdrücklich vor gefälschten Links zu seinem Forum und befürwortet die Verwendung eines benutzerdefinierten Plugins, um solche Betrügereien zu erkennen:

Abbildung 7: Betrugswarnung von Verified

In ähnlicher Weise veröffentlicht BreachForums eine Liste aller seiner legitimen Domänen sowie einen monatlichen „Transparenzbericht“, um zu bestätigen, dass die Website und die zugehörige Infrastruktur unter seiner Kontrolle bleiben und nicht kompromittiert wurden (obwohl dies wahrscheinlich auch eine Vorsichtsmaßnahme ist Maßnahme aufgrund dessen, was mit RaidForums passiert ist):

Abbildung 8: Einzelheiten zum monatlichen Transparenzbericht von BreachForums

Aber Schlichtungsstellen sind die Hauptmethode für den Umgang mit Betrug. Der Prozess ist relativ einfach. Benutzer, die einen Betrug melden möchten, müssen einen neuen Thread erstellen, den Benutzer anrufen, der sie angeblich betrogen hat, und so viele Details wie möglich über den Vorfall

angeben. BreachForums stellt hierfür eine Vorlage bereit, während XSS lediglich die erforderlichen Details auflistet.

Abbildung 9: Vorlage für Betrugsberichte von BreachForums

Abbildung 10: Die in XSS-Betrugsberichten erforderlichen Daten: Benutzername, Link zum Profil, Kontaktdaten, Beweise (Chatprotokolle, Screenshots, Brieftaschen, Überweisungen), alle zusätzlichen Informationen

Ein Moderator überprüft dann den Bericht, bittet um weitere Informationen, falls erforderlich, markiert den Angeklagten und gibt ihm eine Frist für die Antwort (normalerweise 24 Stunden, kann aber zwischen 12 und 72 Stunden liegen).

Abbildung 11: Ein Exploit-Moderator gibt einem beschuldigten Betrüger 24 Stunden Zeit, um auf einen Vorwurf zu reagieren

Der Angeklagte kann die Forderung akzeptieren, in diesem Fall leistet er dem Opfer Wiedergutmachung. Das ist selten. Häufiger bestreitet der Angeklagte die Behauptung (in diesem Fall entscheidet der Moderator) oder antwortet überhaupt nicht (in diesem Fall kann er vorübergehend oder dauerhaft aus dem Forum ausgeschlossen werden).

Abbildung 12: Ein umstrittener Anspruch auf XSS in Bezug auf AaaS-Angebote

Bei strittigen Behauptungen kann der Moderator für eine Partei entscheiden oder entscheiden, dass aufgrund fehlender Beweise kein Fall zu beantworten ist. In einigen Fällen erhalten eine oder beide Parteien Verwarnungen oder vorübergehende oder dauerhafte Sperren.

Abbildung 13: Der Administrator von BreachForums schließt einen Betrugsbericht aufgrund fehlender Beweise

Abbildung 14: Ein umstrittener Anspruch auf Exploit bezüglich eines Crypters zur Verwendung mit Remcos

Diese Diskussionen sind manchmal zivil und werden gütlich zur Zufriedenheit beider Parteien beigelegt. Wir haben ein Beispiel notiert, bei dem der Schiedsrichter entschied, dass der Angeklagte 50 % des geforderten Betrags zurückzahlen sollte:

Abbildung 15: Ein Exploit-Moderator gibt dem Angeklagten 24 Stunden Zeit, um 50 % des geforderten Betrags zurückzuzahlen

In einem Fall entschädigte der Administrator von BreachForums sogar ein Betrugsopfer aus eigener Tasche:

Abbildung 16: Der Administrator von BreachForums entschädigt ein Betrugsopfer persönlich mit 200 US-Dollar

Betrugsberichte enden jedoch häufiger in Beleidigungen und Gegenanschuldigungen. In einigen Fällen wurden die mutmaßlichen Opfer später selbst wegen Betrugs gesperrt.

Abbildung 17: Ein Betrugsbericht über Exploit führt dazu, dass der Ankläger den Ankläger des Betrugs beschuldigt

Folgen

Verbote (und in geringerem Maße Verwarnungen) scheinen das häufigste Ergebnis in Schiedsverfahren zu sein, aber BreachForums verfolgt einen etwas anderen Ansatz. Vielleicht, um zukünftige Betrüger abzuschrecken, veröffentlichen die Moderatoren die Registrierungs-E-Mail-Adressen und

Registrierungs- und zuletzt gesehenen IP-Adressen gesperrter Benutzer, wodurch sie teilweise doxiert werden:

Abbildung 18: Ein Beispiel eines gesperrten Benutzers, komplett mit veröffentlichter Registrierungs-E-Mail-Adresse, Registrierung und letzten bekannten IP-Adressen

Wir haben einige Fälle von Serienbetrügern bemerkt, die nach einer Sperrung einfach ein neues Profil mit einer neuen Identität erstellten, eine neue Registrierungsgebühr zahlten und wieder mit dem Betrügen begannen.

Nicht nur kleine Gauner

Wir haben einige Beispiele notiert, an denen prominentere Bedrohungsakteure beteiligt waren. Hier ist zum Beispiel ein merkwürdiger Fall, der nicht so sehr ein Betrug war, sondern einen Benutzer betraf, der im Namen eines Opfers mit der Conti-Ransomware-Gruppe verhandeln wollte:

Abbildung 19: Ein Benutzer erhebt eine Schiedsklage, um zu versuchen, mit der Conti-Gruppe über die Entschlüsselung der Vermögenswerte eines Unternehmens zu verhandeln

Dieser Bericht wurde von Exploit-Moderatoren geschlossen, da er sich auf Ransomware bezog, die angeblich in diesem Forum verboten ist. Interessant ist jedoch, dass der Beschwerdeführer selbst ein Bedrohungsakteur zu sein scheint und dem Exploit-Forum über drei Jahre lang beigetreten war, bevor er den oben genannten Anspruch geltend machte – mit mehreren Beiträgen, in denen er sein Interesse am Kauf von Daten bekundete. Ihre Beziehung zu Contis Opfer in diesem Fall ist nicht klar.

Abbildung 20: Einige der früheren Beiträge des Beschwerdeführers im Exploit-Forum

Ein weiterer Fall betraf „Alan Wake“ (ein Name aus einem Videospiel), der den letzten Wettbewerb auf XSS gesponsert hatte und zuvor von einem Lockbit-Betreiber beschuldigt wurde, der Anführer der Ransomware-Gruppen Conti und BlackBasta zu sein . Ein Benutzer beschuldigte Alan Wake, sein Gehalt nicht gezahlt zu haben, weil er „Verkehr aus Muscheln gemacht“ habe:

Abbildung 21: Der XSS-Betrugsbericht gegen „Alan Wake“

Alan Wake bestritt den Vorwurf, und der Fall wurde vom Administrator geschlossen und der Beschwerdeführer gesperrt – nicht wegen Betrugs, sondern wegen „Beleidigungen, Angriffen, Drohungen usw.“ und „äußerst unangemessenem Verhalten“.

Schließlich wurde All World Cards (ebenfalls ein früherer Sponsor von XSS-Wettbewerben), eine prominente Carding-Gruppe, selbst Opfer eines Betrugs mit einer gefälschten Schwachstelle und verlor 2000 USD.

Abbildung 22: Die Gruppe All World Cards meldet einen Betrug, bei dem sie 2000 Dollar verloren hat

Wenn es eine Erkenntnis aus all dem gibt, dann die, dass kein Benutzer immun ist; Jeder Handel in kriminellen Foren birgt ein inhärentes Betrugsrisiko. Obwohl es sowohl proaktive (Warnungen, Plugins, Garanten) als auch reaktive (Schlichtungsstellen) Maßnahmen gibt, sind Betrüger nicht nur üblich, sondern – nach den von uns gesammelten Daten zu urteilen – oft erfolgreich. Einer der Gründe für ihren Erfolg ist die schiere Vielfalt der Betrügereien, die sie ziehen.

Im zweiten Teil unserer Untersuchung, der nächste Woche um diese Zeit (Mittwoch, 14. Dezember) erscheinen wird, behandeln wir die verschiedenen Arten von Betrug, die wir beobachtet haben.

Managed Security Services: 4 kritische Fragen, die Sie stellen sollten

Die Landschaft der Cybersicherheitsbedrohungen ist unglaublich volatil. Cyberkriminelle gehen immer professioneller vor, spezialisieren sich zunehmend und treten sogar in Konkurrenz zu anderen Grup…

Managed Security Services: 4 kritische Fragen, die Sie stellen sollten

Verfasst von Jörg Schindler

24. November 2022

Die Landschaft der Cybersicherheitsbedrohungen ist unglaublich volatil. Cyberkriminelle gehen immer professioneller vor, spezialisieren sich zunehmend und treten sogar in Konkurrenz zu anderen Gruppierungen. In der Folge sind Unternehmen innerhalb von Monaten, Wochen oder Tagen – manchmal sogar gleichzeitig – nicht nur einmal sondern immer wieder Angriffen ausgesetzt.

Der weltweite Arbeitskräftemangel im Bereich Cybersicherheit verschärft diese Herausforderungen. Weltweit hat sich die Personallücke im Bereich Cybersicherheit im Jahr 2022 nach Angaben der „2022 Cybersecurity Workforce Study by (ISC)²“ um 26,2 % erhöht, mit insgesamt mehr als drei Millionen offenen Stellen. Während einige Regionen besser abschneiden als andere – wie beispielsweise Lateinamerika, das die Lücke um 26,4 % schloss – bergen die verbleibenden Engpässe immer noch nationale Sicherheitsrisiken.

Cyberkriminelle sind immer aktiv, und Sicherheitsteams müssen es auch sein. Viele Organisationen, die nicht über die

erforderlichen Ressourcen verfügen, um selbst immer komplexere Cyberbedrohungen zu erkennen und darauf zu reagieren, entscheiden sich für die Nutzung von Cybersecurity-as-a-Service (CSaaS), um proaktive Abwehrmaßnahmen zu implementieren. Beim CSaaS-Modell setzen Unternehmen externe Spezialisten ein, um kritische Cybersicherheitsanforderungen zu erfüllen, wie z. B. Bedrohungsüberwachung rund um die Uhr. Durch die Auslagerung oder Erweiterung von IT-Teams mit Managed Detection and Response (MDR)-Services als zentrales CSaaS-Angebot können Unternehmen dazu beitragen, Angriffe abzuschwächen, bevor sie auftreten. Jedes Unternehmen, das erwägt, den Sicherheitsbetrieb auszulagern, sollte Sicherheitsdienstpartnern diese vier Fragen stellen:

1.Welche Erfahrung haben sie in der Zusammenarbeit mit anderen Unternehmen in unserer Branche und Region?
Wenn der Anbieter mit anderen Organisationen in ihrer Branche und Region zusammenarbeitet, sollten diese über Erfahrungen aus erster Hand bei der Verteidigung gegen die spezifischen Bedrohungen verfügen, denen sie ausgesetzt sind.

2. Können sie unsere bestehenden Technologien verwalten und unterstützen?
Fragen sie, ob der CaaS-Anbieter auf ihren vorhandenen Sicherheitstechnologien aufbauen kann, oder ob sie das, was sie bereits im Einsatz haben, entfernen und ersetzen müssen. Der ideale Anbieter sollte in der Lage sein, mit den vorhandenen Technologielösungen zu arbeiten.

3. Wie ausgereift ist ihr Verständnis von neu auftretenden Cyberbedrohungen?
Kriminelle entwickeln sich häufig in den Taktiken, Techniken und Verfahren (TTPs) weiter, die sie verwenden, um Angriffe möglichst unbemerkt durchzuführen. Unternehmen sollten sehr sorgfältig darauf achten, dass ein potenzieller Anbieter die entsprechenden Ressourcen vorweisen kann, mit denen er eine qualitativ hochwertige Bedrohungsanalyse sowie schnelle Reaktion gewährleisten kann.

4. Kann die Lösung eines potenziellen Partners mit unserem Unternehmen skalieren und sich mit unseren Anforderungen weiterentwickeln?
Es ist von entscheidender Bedeutung, dass jeder potenzielle Partner in der Lage ist, den individuell wachsenden und sich entwickelnden Anforderungen gerecht zu werden und die Unternehmenssicherheit zusammen mit sich ändernden Anforderungen effektiv zu optimieren.

Mit einem starken CSaaS-Anbieter sind Unternehmen in der Lage, eine vollständig etablierte Sicherheitsstruktur mit proaktiven Abwehrmaßnahmen und 24/7-Unterstützung zur realisieren. Dies gibt Unternehmen die Möglichkeit, ihre IT-Operationen kontinuierlich zu verbessern und Organisationsmodelle zu verfeinern, wodurch sie in einer äußerst volatilen Bedrohungslandschaft nicht nur überleben, sondern auch wachsen können.

Black Hat

Black Hat

Betrüger, die Betrüger betrügen, Hacker, die Hacker hacken: Erkundung einer verborgenen Subökonomie in Foren und Marktplätzen für Cyberkriminalität

Matt Wixey | Leitender technischer Redakteur, Sophos
Angela Gunn | Senior Threat Researcher / Cybersecurity Writer, Sophos

Datum : Mittwoch, 7. Dezember | 15:20-16:00 Uhr (Capital Suite Zimmer 7/12 (Ebene 3))

Format : 40-Minuten-Briefings

Spuren : Menschliche Faktoren, Verteidigung Es ist kein Geheimnis, dass kriminelle Foren und Marktplätze mit schändlichen Aktivitäten vollgestopft sind. Aber hinter all den Initial Access Brokern, gestohlenen Daten und Malware gibt es eine versteckte, blühende Unterkategorie der Kriminalität, die unbemerkt bleibt: Bedrohungsakteure, die es auf andere Bedrohungsakteure abgesehen haben. Diese kannibalischen Kriminellen (wir nennen sie „Metaparasiten“: ein Parasit, dessen Wirt auch ein Parasit ist) sind ein so hartnäckiges und teures Problem, dass es spezielle Forenräume gibt – die Tausende von Posts enthalten und Jahre zurückreichen –, die dafür bestimmt sind, sie auf die schwarze Liste zu setzen und Betrug zu schlichten Beschwerden zwischen Benutzern und das Melden von nachgeahmten „Ripper“-Sites. In diesem Vortrag präsentieren wir eine neuartige Untersuchung über Betrüger, die Betrüger betrügen, und Hacker, die Hacker hacken, auf drei der etabliertesten und bekanntesten kriminellen Marktplätze. Wir untersuchen die Größe dieses schattigen Multi-Millionen-Dollar-Ökosystems; die Beweggründe von Metaparasiten; wie Schiedsverfahren funktionieren; und welchen Einfluss Metaparasiten auf die Kultur und den Betrieb der Marktplätze haben, auf denen sie tätig sind. Anschließend tauchen wir tief in Fallstudien ein und betrachten die Techniken, die Metaparasiten verwenden, von altmodischem „Rip and Run“-Betrug und gefälschten Datenlecks bis hin zu ausgeklügelten Phishing-Kampagnen, Verweisbetrug, Typosquatting und Backdoor-Malware. Unterwegs decken wir einen groß angelegten, koordinierten und lukrativen Betrug auf, an dem ein Netzwerk von 15 gefälschten Marktplätzen beteiligt ist, und Fälle, in denen sich die Bedrohungsakteure rächen und die Betrüger betrügen, die sie betrogen haben. Sie könnten fragen: Wen kümmert es, wenn Kriminelle sich gegenseitig abzocken? Aber Metaparasiten bieten Analysten unbeabsichtigt einen Informationssegen, der es uns ermöglicht, beispiellose Einblicke in Verkäufe, Operationen, Verhandlungen und Identifikatoren zu gewinnen,

die sonst verborgen bleiben würden – sowie in die Marktkultur, unterschiedliche Ebenen der Betriebssicherheit und Anfälligkeit für Täuschung und Sozialtechnik. Unser Vortrag wird auch dazu beitragen, Analysten und allgemein Neugierige davor zu schützen, versehentlich auf einige dieser Betrügereien hereinzufallen, wenn sie kriminelle Marktplätze untersuchen.

Präsentationsmaterial

- Folien hier herunterladen

EU verabschiedet NIS2-Richtlinie – Umsetzung bis 2024

Nach dem EU-Parlament hat auch der EU-Rat der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS2) zugestimmt. Die Mitgliedsstaaten müssen sie bis Herbst 2024 in nationales Recht umsetzen. Sie soll die Resilienz und die Kapazitäten zur Reaktion auf Sicherheitsvorfälle sowohl des öffentlichen als auch des privaten Sektors und der EU als Ganzes weiter verbessern. Die NIS2-Richtlinie steht im Zusammenhang mit zahlreichen gesetzgeberischen Maßnahmen im Bereich IT- und Cybersicherheit.

Ähnlich den Vorgaben der KRITIS-Verordnung werden Unternehmen betroffener Branchen verpflichtet, Risikomanagementmaßnahmen zu ergreifen und Meldepflichten zu beachten. Zu den Branchen zählen unter anderem Energie, Verkehr, Gesundheit und digitale Infrastruktur. Um sicherzustellen, dass nur mittlere und große Unternehmen von den Vorgaben erfasst werden, sieht die Richtlinie Schwellenwerte für ihre Anwendbarkeit vor.

Ziel der Richtlinie ist eine Harmonisierung der einschlägigen Bestimmungen in den einzelnen EU-Staaten durch Mindestvorgaben und Regeln zur wirksameren Zusammenarbeit zwischen den

nationalen Behörden. Unter anderem bei Aspekten der Zusammenarbeit und Kooperation sowie den Anforderungen an das Cybersecurity-Risikomanagement geht die Richtlinie deutlich über die NIS1-Richtlinie hinaus. *Tobias Haar* (ur@ix.de)

Kurz notiert

Aagon veröffentlicht ein Produkt zum **BitLocker-Management.** Es bietet die zentrale Verwaltung des Windows-Bordmittels zur Festplattenverschlüsselung sowie Monitoring- und Reportfunktionen.

Seit Kurzem stehen 102 Vorträge der diesjährigen **Sicherheitskonferenz Black Hat** auf dem YouTube-Channel des Veranstalters zum Nachschauen bereit (siehe ix.de/zey7).

Der **verinice.veo-Datenschutzmanager** steht Interessierten in einer Einzelplatz-Betatestversion zur Verfügung. Mit dem Datenschutzmanagementsystem lassen sich die Vorgaben der DSGVO verwalten und ihre Umsetzung gewährleisten.

Ungepatchte Schwachstelle im WordPress-Core: Was es wirklich bedeutet

Geschrieben von iThemes-Redaktionsteam an 14. Dezember 2022

Zuletzt aktualisiert am 14. Dezember 2022

Diese Woche Im iThemes Vulnerability Report werden Sie feststellen, dass es eine ungepatchte Schwachstelle im WordPress-Core gibt. Diese Schwachstelle wurde von Thomas Chauchefoin gemeldet und betrifft derzeit alle Versionen von

WordPress. Die wahrscheinliche Ausnutzung dieser Schwachstelle ist jedoch sehr gering, und um sich vollständig zu schützen, müssen Sie lediglich XML-RPC oder Pingbacks auf Ihrer WordPress-Site deaktivieren.

Was diese Schwachstelle für Ihre Website bedeutet

Obwohl ein vollständiger Proof of Concept noch nicht von WPScan veröffentlicht wurde, können wir einige fundierte Vermutungen darüber anstellen, wie diese Schwachstelle ausgenutzt werden kann. Sie sagen:

> *„WordPress ist von einer nicht authentifizierten blinden SSRF in der Pingback-Funktion betroffen. Aufgrund einer TOCTOU-Rennbedingung zwischen den Validierungsprüfungen und der HTTP-Anfrage können Angreifer interne Hosts erreichen, die ausdrücklich verboten sind.“*

Um diese Schwachstelle auszunutzen, würde ein Angreifer WordPress-Pingbacks verwenden, wäre aber dazu gezwungen, dies in Kombination mit anderen Schwachstellen zu tun.

Um eine Schwachstelle wie diese auszunutzen, um einer WordPress-Site irgendeinen Schaden zuzufügen, wäre diese Schwachstelle nur nützlich, wenn sie mit anderen ernsteren Schwachstellen auf einer nicht gepatchten oder unsicheren WordPress-Site verwendet wird.

Offiziell hat das Sicherheitsteam von WordPress.org erklärt, dass es sich um eine Schwachstelle mit niedriger Priorität handelt. Insbesondere sagten sie dem Daily Swig :

> *„… dies ist ein Problem mit geringen Auswirkungen, und um es auszunutzen, muss es mit zusätzlichen Schwachstellen in Software von Drittanbietern [verkettet] werden. Daher betrachtet das Sicherheitsteam das Problem als gering.“*

Sie fügten hinzu: „Aufgrund seines geringen Schweregrades diskutiert das Team, ob dieses Problem als allgemeine Härtungsmaßnahme öffentlich behoben werden könnte.“

Dies unterstreicht die Schwierigkeit, Sicherheitsfixes zu so vielen älteren Versionen von WordPress hinzuzufügen. Jahrelang hat das Kernteam Patches auf Versionen zurückportiert, die viele Jahre alt waren und nur von wenigen Nachzüglerseiten verwendet wurden, die noch nicht aktualisiert wurden. Die jüngste Entscheidung des Kernteams, ältere Versionen nicht mehr zurückzuportieren, wird die Behebung dieser Art von Problemen für das WordPress-Kernteam einfacher und schneller machen.

So schützen Sie Ihre Website

Da Pingbacks der offensichtliche Schwachpunkt sind, der diskutiert wird, ist das Deaktivieren von Pingbacks und/oder XML-RPC ein guter erster Schritt.

Wenn Sie Ihre WordPress-Site auf dem neuesten Stand halten und sich auf einem zuverlässigen Hosting mit einer starken und sicheren Infrastruktur befinden, ist die Wahrscheinlichkeit einer Ausnutzung dieser Schwachstelle extrem gering.

Wenn Sie Ihre Website so sicher wie möglich halten möchten, ist es am besten, Pingbacks oder XML-RPC zu deaktivieren. Glücklicherweise bietet Ihnen iThemes Security die Möglichkeit, beides zu tun.

So deaktivieren Sie XML-RPC mit iThemes Security

Das Deaktivieren von XML-RPC mit iThemes Security ist unglaublich einfach. Gehen Sie zu **Sicherheit > Einstellungen > Erweitert > WordPress-Optimierungen** und verwenden Sie dann das Dropdown-Menü, um XML-RPC zu deaktivieren.

Es kann Fälle geben, in denen Sie XML-RPC benötigen. Diese beinhalten:

- Wenn Sie eine alte Website haben, die Sie nicht auf Version 4.4 oder höher aktualisieren können, haben Sie keinen Zugriff auf die REST-API und verwenden möglicherweise Dienste, die XML-RPC erfordern.
- Sie verwenden ein Programm, das nicht auf die REST-API zugreifen kann, um mit Ihrer Website zu kommunizieren.
- Integration mit einigen Apps von Drittanbietern, die nur XML-RPC verwenden können.

Das Deaktivieren von XML-RPC ist mit iThemes Security ein einfacher Vorgang. Sie können dies ausschalten und die Funktionalität Ihrer Website testen, und wenn etwas nicht richtig zu funktionieren scheint, können Sie es wieder einschalten.

Dies sind Situationen, in denen es sinnvoll ist, einen Staging-Server einzurichten, damit Sie Änderungen testen können, bevor Sie sie auf Ihre Produktionssite anwenden.

Stummschalten der Schwachstelle in Ihrem iThemes Site Scan

Natürlich benachrichtigt Sie der Site-Scanner von iThemes Security über diese Schwachstelle. Da es in naher Zukunft nicht vom Kernteam behoben wird, könnte es sinnvoll sein, der Warnungsermüdung vorzubeugen, indem diese Schwachstelle im Site-Scanner stummgeschaltet wird. Weitere Informationen zum Stummschalten von Schwachstellenwarnungen finden Sie in unserer Hilfedokumentation .

Fazit

Obwohl diese Sicherheitsanfälligkeit nicht gepatcht ist, stellt sie ein sehr geringes Risiko für Besitzer von WordPress-Sites dar. Wenn auf Ihrer Website XML-RPC bereits deaktiviert ist, sind Sie bereits geschützt. Pingbacks sind eine der Legacy-Funktionen von WordPress, die in einigen Fällen nützlich sein können, aber es ist keine Funktion, die von vielen modernen Websites verwendet wird. Dies ist einer der Fälle, in denen es hilfreich ist, ein Sicherheits-Plugin wie iThemes Security installiert zu haben, damit Sie schnell Maßnahmen ergreifen können, um Ihre Website gegen Angreifer zu schützen, selbst wenn die betreffende Schwachstelle von geringer Schwere ist.

VPN-Überblick: Standorte vernetzen, Geoblocking und Zensur umgehen, Privatsphäre schützen

Verschlüsselte Wendungen

Virtual Private Networks gibt es heute für deutlich mehr Zwecke, als der Name vermuten lässt. In diesem Streifzug lesen Sie, wie diese vielfältige Softwaregattung entstand und dass sie neben soliden Ökosystemen auch sumpfige hervorbrachte. Außerdem geht es um Praxis zu einem mächtigen Mauerblümchen.
Virtual Private Networks gibt es heute für deutlich mehr Zwecke, als der Name vermuten lässt. In diesem Streifzug lesen Sie, wie diese vielfältige Softwaregattung entstand und dass sie neben soliden Ökosystemen auch sumpfige hervorbrachte. Außerdem geht es um Praxis zu einem mächtigen Mauerblümchen.

Von Dušan Živadinović

kompakt

- Viele VPN-Anwendungen haben den spröden Charm der Kommandozeile abgelegt und lassen sich komfortabel bedienen.
- Manche neuen VPN-Funktionen spiegeln gut wider, dass Anwendern der freie Internet-Zugang wichtig ist.
- Für den Privatsphärenschutz setzen Entwickler Techniken

ein, die sich bei digitalen Wahlmaschinen bewährt haben.

Ursprünglich hat man Virtual Private Networks (VPN) entwickelt, um entfernte Standorte miteinander zu vernetzen (Site-to-Site), später auch, um ferne Benutzer an Firmen- oder Heimnetze anzukoppeln (Road-Warrior, auch End-to-Site-VPNs genannt), und für diverse andere Zwecke. Zu den wichtigsten davon gehören VPN-Varianten für das Anonymisieren und das Umgehen von Geoblocking und Internet-Sperren (Tor) sowie den Privatsphärenschutz.

Mit Virtual Private Networks waren anfangs nur Routing- und Bridging-Programme zur Standortvernetzung gemeint. Zu Beginn der Internet-Ära koppelte man entfernte Netze sogar noch ohne jeglichen Kryptoschutz. Das änderte sich, nachdem klar wurde, dass über solche Verbindungen auch Daten fließen, die besser vertraulich bleiben.

Fortan blieb die Wahrung der Vertraulichkeit eine der wichtigsten Antriebsfedern und brachte immer neue kryptografische Absicherungen der Nutzdaten gegen unerwünschte Mitleser hervor. Unzureichend gehärtete VPN-Varianten, die ihre vertrauliche Fracht nicht vor Angreifern schützen konnten, verschwanden wieder von der Bildfläche. Ein Beispiel ist das von Microsoft entwickelte Point-to-Point Tunneling Protocol (PPTP), das zwar sehr einfach zu konfigurieren war, sich aber mit überschaubarem Aufwand knacken ließ (siehe ct.de/y9y1). PPTP hat in modernen Installationen nichts zu suchen.

Neben PPTP kamen diverse Spielarten von SSL-VPNs auf und erlangten große Verbreitung. Sie verschlüsseln Nutzdaten mittels Transport Layer Security (früher Secure Socket Layer, SSL, genannt). Bis heute sehr verbreitet sind Implementierungen, die ohne Clientsoftware funktionieren, weil sie sich besonders für den spontanen Aufbau gesicherter Verbindungen eignen (Tunnel), also etwa zwischen Webbrowsern

und Webservern. Viele tunneln aber nur den Verkehr bestimmter Anwendungen (z. B. Mailclient und -server, verschlüsselnde DNS-Clients und -Resolver), bieten also keine Infrastrukturvernetzung etwa für Dateifreigaben, weshalb ihre Einordnung zu VPNs umstritten ist.

Die bekannteste SSL-VPN-Spielart inklusive Netzwerkzugriff, also mit Kapseln kompletter IP-Pakete, ist bis heute das quelloffene OpenVPN. Jahrelang galt es als das am weitesten verbreitete VPN überhaupt. Daneben gibt es diverse weniger bedeutende SSL-VPNs etwa von Router-Herstellern wie Netgear. Neben OpenVPN galten lange Zeit nur das komplizierte, aber bis heute sichere IPsec und Varianten wie IPsec/L2TP als zuverlässige Alternative zur Netzwerkkopplung.

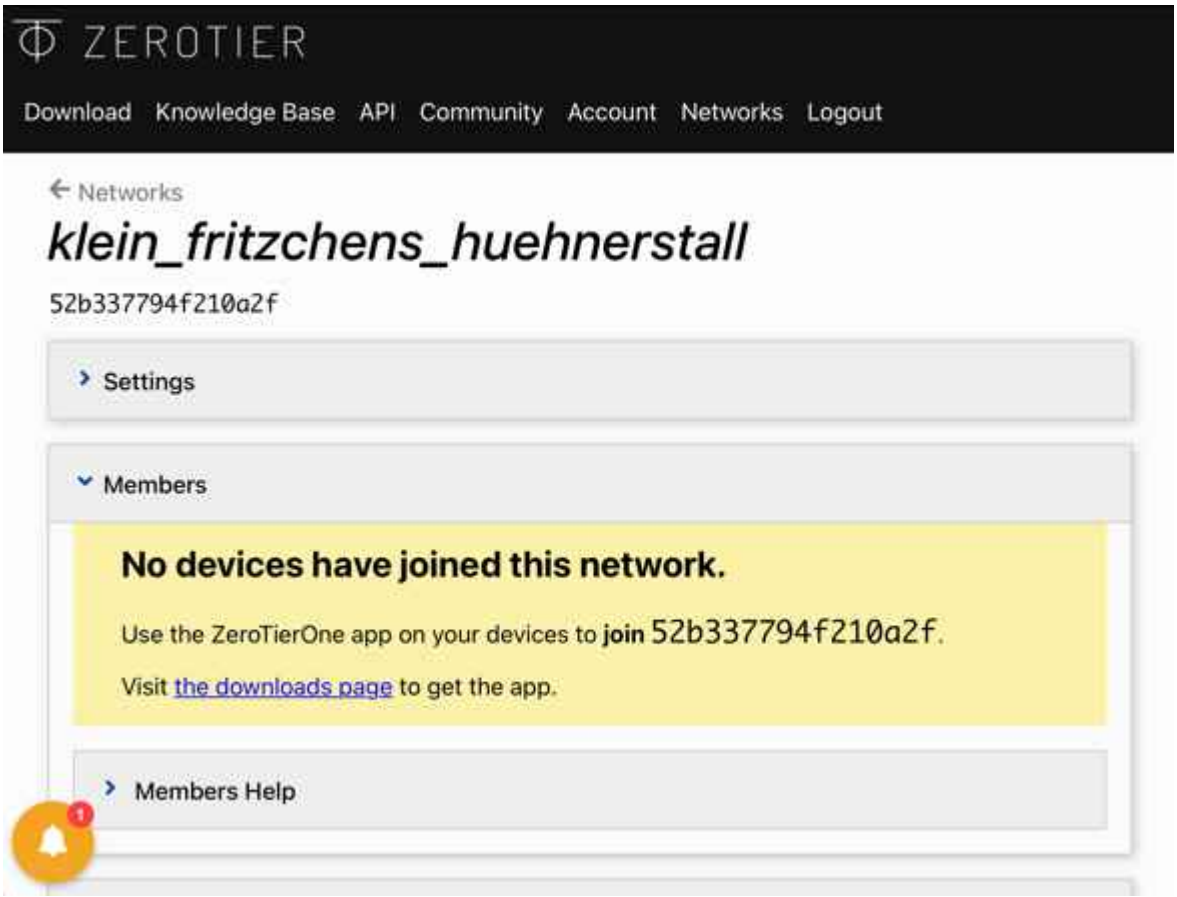
Auf der Beliebtheitsskala rangiert vor OpenVPN inzwischen das 2019 erschienene, ebenfalls quelloffene WireGuard, das auch schneller ist als OpenVPN & Co. Anders als OpenVPN und andere VPN-Verfahren klammert WireGuard die Benutzerverwaltung komplett aus und regelt nur die Vernetzung und das Chiffrieren von Nutzdaten mittels kryptografischer Schlüsselpaare. Wer sich für Implementierungsdetails interessiert, findet bei der Internet Engineering Task Force (IETF) eine Zusammenfassung für gängige VPNs, darunter TLS, IPsec und WireGuard (ct.de/y9y1). Beispiele für interessante, aber wenig verbreitete VPN-Varianten sind Nebula, SoftEther, Tinc, Twingate oder auch tinyfecVPN (dank spezieller Fehlerkorrektur empfehlenswert für gestörte Leitungen).

Netzwerkkopplung mit Komfort

Wer einfach nur von unterwegs auf einen Server im Heimnetz zugreifen will, den stellen die üblichen VPN-Anwendungen vor zu hohe Hürden. An diesem Punkt kommen VPN-Dienste ins Spiel, die man mittels vereinfachter Programme im Handumdrehen

verwenden kann. Zu den ersten Vertretern gehört das kostenpflichtige LogMeIn Hamachi, das sich nach dem Start über die Firewall des Heimrouters hinweg bei der Infrastruktur des Anbieters anmeldet. Anschließend können Hamachi-Clients laut dem Hersteller direkt miteinander kommunizieren (automatisches NAT-Traversal), also ohne den Umweg über Hamachi-Server. Bisher hat der Hersteller den Quellcode aber nicht veröffentlicht, sodass man weder die Sicherheit noch die Funktionsweise prüfen kann.

Zu den komfortablen, aber quelloffenen und geprüften VPNs gehören der WireGuard-Abkömmling Tailscale und ZeroTier. Mit ZeroTier verknüpft man Netzwerkgeräte über einen virtuellen Managed Switch, den ZeroTier anbietet (den man mit Abstrichen aber auch selbst betreiben kann) und der einfach per Web-Interface konfiguriert wird.



Als ZeroTier-Admin koppelt man PCs oder Smartphones innerhalb von Minuten in ein virtuelles Netzwerk. Wer den Dienst ausprobieren möchte, kann gratis eine Handvoll Netzwerke aufsetzen und Clients nach Belieben hinzufügen und entfernen.

Fortgeschrittene können ZeroTier-Gateways einrichten, die zwischen einem virtuellen Netz und einem physischen vermitteln.
Auf Linux, macOS, Windows, Android und iOS klappt das Einrichten mit geringem Aufwand, für den Verbindungsaufbau der Clients muss der UDP-Port 9993 geöffnet sein (alternativ UPnP für die beteiligten Hosts im Router einschalten). Das Web-Interface bietet zahlreiche Optionen, die sich an fortgeschrittene Admins richten. Beispielsweise kann man Subnetze beinahe nach Belieben wählen, öffentliche oder private Netze bilden, Netzwerkteilnehmern mehr als eine IP-Adresse und spezielle DNS-Resolver zuweisen oder Clients per Hand aus dem Netz kicken. ZeroTier ist quelloffen und von Fachleuten geprüft und für sicher befunden.

Stille VPNs

VPN-Funktionen verstecken sich manchmal an ungewöhnlichen Stellen. Das ist beispielsweise der Fall bei hybriden Internet-Anschlüssen. Dabei fasst ein Router im Zusammenspiel mit einem Hub im Rechenzentrum per VPN mehrere Internet-Leitungen zu einem Bündel zusammen, was die summierte Datenrate erhöht und die Ausfallsicherheit verbessert. Die Deutsche Telekom bietet solche Anschlüsse unter dem Namen „Magenta zu Hause Hybrid“ an. Dabei wird je ein DSL- und ein Mobilfunk-Zugang gebündelt. Der Router-Hersteller Viprinet bündelt beliebige Internet-Zugänge, ob DSL, Glasfaser, Kabel oder Mobilfunk.

Eine berüchtigte Gruppe unter den VPN-Anwendungen bilden Programme für das Peer-to-Peer-File-Sharing. Dabei versteckt die Sicherungsschicht die Nutzdaten. Manche Anwender verbreiten über diese Softwareklasse, die Napster begründet hat, illegal Medien und Programme. Das Piraten-Image haftet zwar weiter an, aber über Anwendungen wie BitTorrent werden etwa Linux-Distributionen weltweit kostengünstig verteilt und Unternehmen wie Microsoft nutzen die Technik, um Updates oder Spiele-Elemente zu verbreiten (z. B. beim Online-Rollenspiel

Skyforge).

Umgehung per Tunnel

Mit Aufkommen der Videostreamingangebote teilten vor allem US-amerikanische Medienhäuser den Weltmarkt in Regionen auf, um ihre Kommerzialisierungsideen durchzusetzen. Dafür werten deren Server den Standort der Nutzer aus: Wer aus einem noch nicht bedienten Gebiet anfragt, bekommt nichts zu sehen (Geoblocking). Filterkriterien sind beispielsweise die IP-Adressen der Nutzer und der Standort des befragten DNS-Resolvers, der den Anwendern beim Verbindungsaufbau die IP-Adresse der Streamingserver mitteilt. So bleiben etwa die Tore von HBO geschlossen, wenn man sich aus Europa anmeldet.

Mit VPN-Anwendungen täuscht man legitime Standorte vor, indem man den fernen Tunnelendpunkt in ein Land legt, das der Streaminganbieter versorgen will, also etwa in die USA. Ein derartiges VPN kann man mit etwas Know-how selbst basteln, indem man den VPN-Server in einer Cloud installiert, vorausgesetzt, man kann dessen Standort wählen. Solche Angebote kosten bei Amazon oder DigitalOcean monatlich wenige Euro. Zusätzlich muss das Betriebssystem des Nutzers einen Resolver aus dem Zielland befragen, sodass man auch diesen auf dem Cloudserver einrichtet oder einen offenen Resolver ausfindig macht, der im Zielland steht.

Privatsphärenschutz

Für jedes ferne Tunnelende braucht man aber einen separaten Server, sodass es schnell teuer wird, wenn man mehrere Endpunkte braucht. Deshalb, und auch weil die VPN-Konfiguration nicht jedermanns Sache ist, kamen vor einigen Jahren VPN-Anbieter auf den Markt, die genau dieses Anwendungsfeld mit eigenen Clients abdecken. Darüber kann man vor jedem Verbindungsaufbau einen von meist vielen Tunnelendpunkten per Menü auswählen.

Zusätzlich versprechen die Diensteanbieter, die Privatsphäre zu schützen, denn ohne VPN können Angreifer oder Spione Metadaten wie Ziel-Domains, Quell- und Ziel-IP-Adressen und unverschlüsselten Verkehr zum Beispiel an WLAN-Hotspots abfischen. Staatliche Sicherheitsorgane können solche Daten auch an Internet-Austauschknoten abgreifen.

Ein VPN schützt die Meta- und Nutzdaten kryptografisch, solange die Daten vom Nutzer zum Tunnelendpunkt unterwegs sind. Die VPN-Clients leiten daher sämtlichen Verkehr über den Tunnel zum VPN-Anbieter, der sie mit seiner eigenen Quell-IP-Adresse zum Ziel ins Internet gibt. Außerhalb des Tunnels erscheint nur die IP-Adresse des VPN-Anbieters. Deshalb lassen sich viele Metadaten nicht mehr korrekt zuordnen, weshalb sie für Angreifer und fremde Sicherheitsorgane wertlos sind.

Das gilt aber nicht für den Betreiber des VPNs, denn er kann den austretenden Verkehr den Nutzern prinzipiell anhand von Tunnel-IDs zuordnen. Deshalb erfordert es großes Vertrauen, ein VPN-Angebot zu buchen. Viele kommerzielle VPN-Anbieter sichern in den AGB zu, die Benutzeraktivitäten nicht zu protokollieren. Aber Kunden können das nicht prüfen. Tatsächlich deutet einiges darauf hin, dass manche Anbieter nur vorgeben, die Privatsphäre zu schützen, sie aber eigentlich sogar aushöhlen.

Sumpfiges Ökosystem

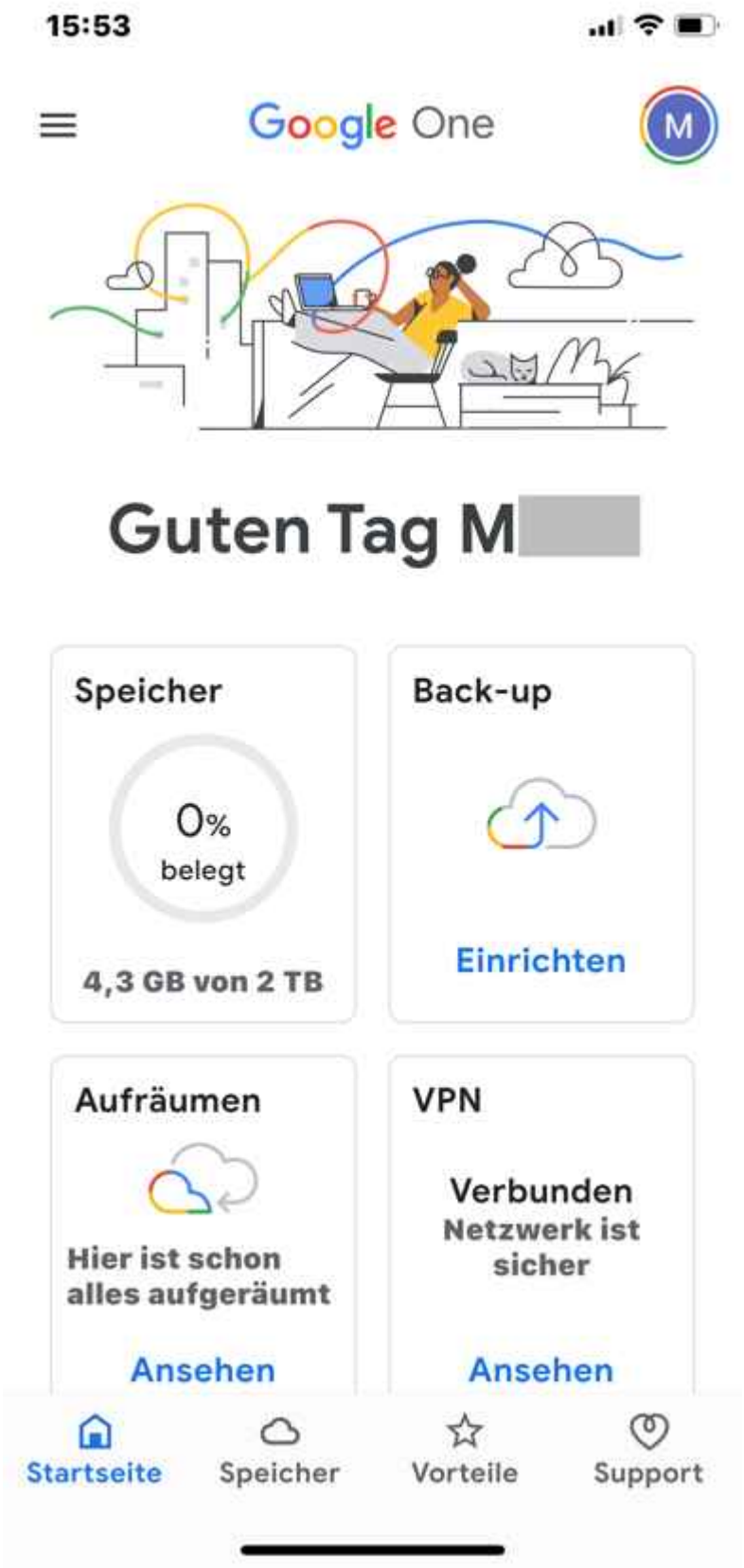
Beispielsweise deckte die Technologieforscherin und Redakteurin Katie Kasunic bereits im Juni 2020 auf, dass 40 VPN-Anbieter nach außen vorgeben, miteinander zu konkurrieren, tatsächlich aber der Kontrolle von nur sieben Unternehmen in Pakistan und China unterstehen. Beispielsweise kontrollierte zum Prüfzeitpunkt die in Singapur ansässige Firma Innovative Connecting insgesamt acht VPN-Anwendungen für Mobilgeräte, deren in China stationiertes Team entwickelte manche der Apps selbst und kontrollierte andere über stillschweigend aufgekaufte Tochterfirmen.

Solche Verflechtungen wecken Zweifel an der Vertrauenswürdigkeit von VPN-Anbietern. Auch erinnern die Firmenkonglomerate daran, dass in China vor einigen Jahren ungewöhnlich viele Tor-Exit-Punkte stationiert wurden. Das weckt den Verdacht, dass der oder die Betreiber am VPN- und Tor-Verkehr interessiert sind. Ein Exit-Node kann mitlesen und weiß lediglich nicht, wer die Daten anfordert. Es ist aber sichtbar, ob Tor-Nutzer zum Beispiel Webseiten abrufen, die einem autoritären Regime unliebsam sind. Auch der Opera-Browser, den manche Nutzer wegen seines eingebauten VPN-Verfahrens schätzen, segelt unter einer fragwürdigen Flagge: Dahinter steht ein Konsortium namens Golden Brick Silk Road Equity Investment Fund, das neben seinem Hauptsitz in China ein Büro in Russland unterhält.

Anscheinend haben also manche restriktiven Regierungen den Spieß umgedreht und nutzen VPNs offensiv zum Bespitzeln ihrer Nutzer. Dabei finanzieren die Bespitzelten durch den Kauf ihre Überwachung unwissentlich selbst.

Großer Entflechtungstrick

Unabhängig von ihrer Redlichkeit haben VPN-Anbieter ein strukturelles Problem: Kundendatenbanken und Verkehrsprotokolle können leicht miteinander verknüpft werden, um auszukundschaften, welche Ziele die VPN-Nutzer im Internet ansteuern. Selbst wenn ein Anbieter keine Log-Funktion eingerichtet hat, könnte er auf staatliche Weisung dazu gezwungen werden, womit die Privatsphäre der User perdu wäre.



Google hat eine eigene VPN-Anwendung für den Privatsphärenschutz entwickelt. Kundendaten und Kundenverkehr sind mittels moderner Kryptografietechniken entflochten.

An dieser Stelle greifen neue Angebote von Apple und Google. Beide entflechten die Authentifizierung der Anwender von den

Verkehrsdaten, sodass sich Benutzernamen und Einwahlzeitpunkte nicht mit IP-Adressen und durchgeleitetem VPN-Verkehr verknüpfen lassen. Dafür setzen beide Konzerne auf RSA Blind Signatures.

Die Technik erlangte in digitalen Wahlmaschinen einige Bekanntheit, weil sich damit digitale Wahlzettel so beglaubigen lassen, dass man die Inhalte keinem Wähler zuordnen kann. Eine Variante der Methode spezifizieren Apple, Cloudflare und Fastly unter dem Dach der Internet Engineering Task Force (siehe ct.de/y9y1).

Google verwendet RSA Blind Signatures beim kostenpflichtigen Dienst „Google One“. Der ist ab monatlich 10 Euro für macOS-, Windows-, Android- und iOS-Clients erhältlich; mit aktuellen Geräten der Pixel-7-Reihe soll der Dienst ab Dezember kostenlos sein. Der Client lenkt den gesamten Verkehr des Smartphones automatisch zum nächstgelegenen Tunnelendpunkt von Google, eignet sich also nicht zur Umgehung von Geoblocking.

Netzwerkverkehr einschließlich DNS, IP-Adressen und Verbindungszeiten werden Google zufolge nicht protokolliert, was den Dienst attraktiv erscheinen lässt. Wie bei anderen VPNs können auch hier Dritte im Datenstrom schnüffeln, sobald er den Tunnel verlassen hat, sodass man darauf achten muss, keine unverschlüsselten Anwendungen zu verwenden.

Die VPN-Varianten für Windows und macOS sind noch sehr frisch. Auf Android und iOS haben wir den Dienst ausgiebig getestet und dabei fielen nur wenige Fehlversuche auf. Der VPN-Client baut den Tunnel (vermutlich für Stromsparzwecke) häufig ab und bei Bedarf wieder auf und meldet jeden Statuswechsel. Wer das lästig findet, kann das Meldungsfeuer abschalten. Doch ob Sie ausgerechnet der Datenkrake Google auch noch fürs VPN vertrauen sollten, sei dahingestellt.

Apples Privatsphärenschutz Private Relay gibt es als Dreingabe zu einem iCloud+-Abo ab 0,99 Euro monatlich. Der Dienst setzt

iOS, iPadOS oder macOS voraus, ist aber ab Werk löchrig: Apple schützt mit Private Relay nicht den gesamten Verkehr des Nutzers, sondern nur den der eigenen Internet-Anwendungen. Dazu gehören DNS-Anfragen und der Verkehr des Safari-Browsers. Statt eines herkömmlichen VPN-Tunnels setzt Apple zwei verkettete Proxies ein (Multi-hop Masque proxy), die unterschiedlichen Betreibern gehören.

Der erste Proxy bekommt verschlüsselte Pakete und weiß daher nicht, welche Domain der Client ansteuern will. Nur der zweite kann sie entschlüsseln und leitet sie zum Ziel weiter, aber er weiß nicht, von welcher Quell-IP-Adresse die Pakete stammen. Deshalb weiß auch ein Webseiten-Betreiber nicht, welche IP-Adresse ein Besucher tatsächlich nutzt. Den ersten Proxy betreibt Apple selbst. Der zweite stammt aus einem Pool, den die CDN-Anbieter Akamai, Cloudflare und Fastly beisteuern. Aus diesem Pool stammen die IP-Adressen, die beim Surfen im Internet sichtbar werden (Test via ct.de/ip). Schaltet man einen VPN-Dienst ein, endet die Umleitung über die Proxies und der Verkehr läuft über den neuen Tunnel.

Wenn Private Relay eine DNS-Anfrage nicht auflösen kann, delegiert es die Aufgabe an den im Betriebssystem konfigurierten Resolver. Auf speziell konstruierten Webseiten wie astrill.com/dns-leak-test sickert so die IP-Adresse des Resolvers durch. Falls das einer ist, der auf Ihren Aufenthaltsort schließen lässt (etwa, weil sie zu Hause einen eigenen betreiben), richten Sie besser den anonymisierenden DNSCrypt-Proxy auf dem Mac ein (siehe ct.de/y46t); der ist auch für Windows und Linux empfehlenswert.

Trotz der Proxy-Kette wirkte Apples Dienst im Test schnell, Verzögerungen im Webseitenaufbau fielen gegenüber dem Betrieb ohne Private Relay nicht auf. Das dürfte daran liegen, dass die Proxies in CDNs stehen, die ohnehin viele nachgefragte Inhalte ausliefern. Im rund sechsmonatigem Test fiel Private Relay nur wenige Male aus und das auch nur vorübergehend. Einige wenige Webseiten, darunter HUK24.de, haben die Proxy-

IP-Adressen fälschlich dem europäischen Ausland zugeordnet und die Anmeldung abgelehnt. Nach Rückmeldungen der Nutzer beseitigten sie das Problem.

Verschleiernde VPNs

Große Firewalls können Datenpakete von gängigen VPNs einschließlich Google One leicht identifizieren und sperren. Auf dieser Grundlage setzen manche Staaten Internet-Zensur durch. Dem stellt eine große Entwicklergruppe das Tor-VPN entgegen. Es verschlüsselt und anonymisiert den Datenverkehr und verschleiert den VPN-Charakter, sodass die Datenpakete beispielsweise wie harmloser HTTP-Verkehr aussehen.

Tor ist hinlänglich bekannt und auch über dessen Snowflake-Erweiterung für Browser, die Tor-Clients zum Weg ins unzensierte Internet verhilft, haben wir berichtet (ct.de/y9y1). Aber da die Datenpakete über mehrere Vermittler ins Internet gelangen, sind sie viel länger unterwegs. Die Tor-Vermittler und der Endpunkt werden zufällig ausgewählt, sodass sich kaum rückverfolgen lässt, von wem eine Internet-Sitzung gestartet wurde. Aber manche restriktiven Regierungen betreiben eigene Tor-Endpunkte und können so mitlesen, welche Seiten im Web aufgerufen werden und Tor-Verkehr manipulieren.

An dieser Stelle kommt das VPN-Mauerblümchen Shadowsocks ins Spiel, das mutmaßlich einer Tastatur in China entstammt. Nachdem der Entwickler 2015 die Arbeit daran aufgeben musste, führten das Projekt andere fort und entwickelten Varianten. Unter diesen sticht das von Googles Jigsaw-Gruppe geführte Projekt Outline hervor. Shadowsocks und Outline standen jahrelang im Schatten von Tor, rückten aber kürzlich durch Netzsperren im Iran in den Blickpunkt.

Shadowsocks

Mit Shadowsocks kann man den Tunnelendpunkt selbst bestimmen, also sicherstellen, dass man keinen unerwünschten Tor-Endpunkt

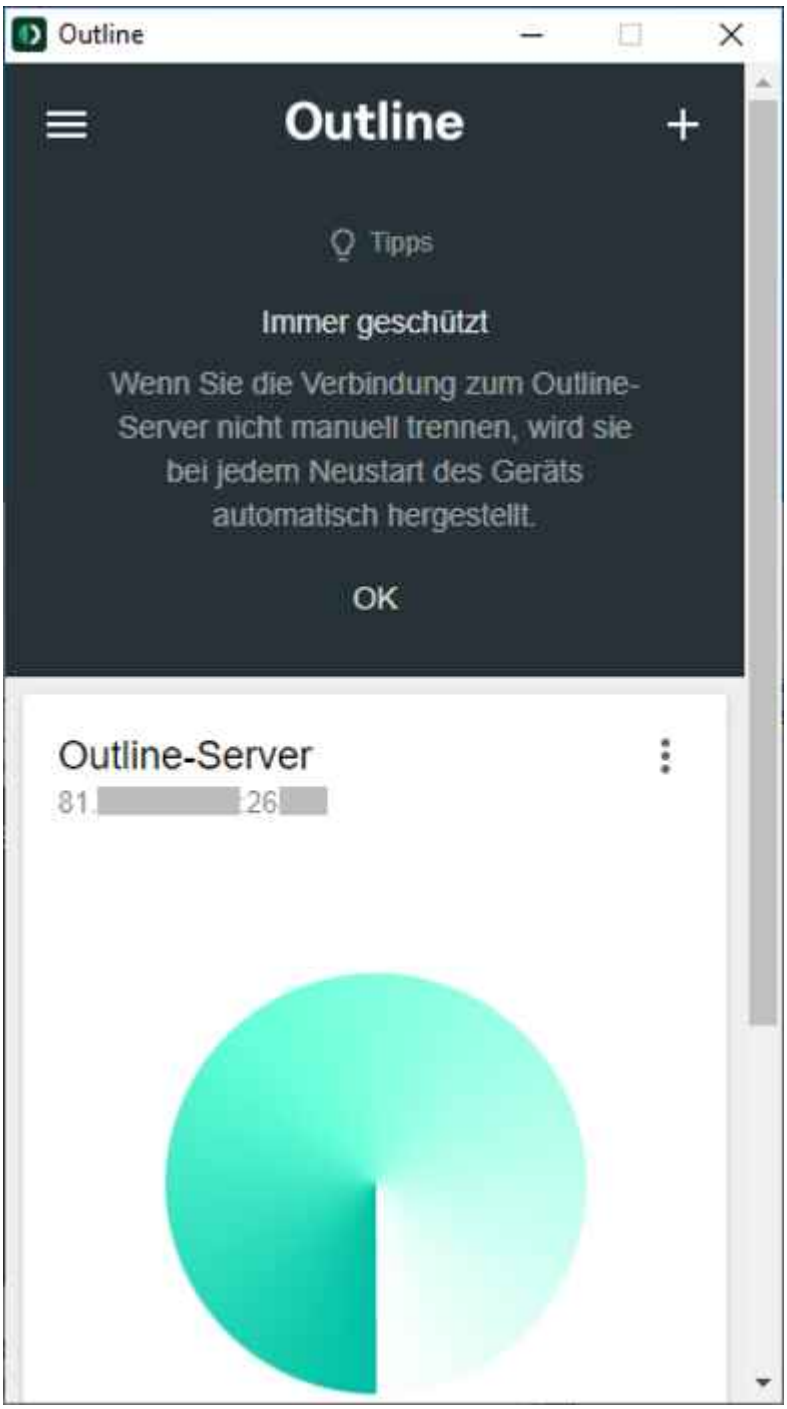
nutzt. Das scheint zwar die Anonymisierung auszuhebeln, weil man für den Server-Betrieb Cloud-Instanzen etwa bei Hetzner anmietet und dabei natürlich Personalien hinterlässt.

Aber manche Betreiber stellen ihre Shadowsocks-Server Nutzern aus dem Iran oder China auf Zuruf incognito und gratis zur Verfügung. Um dann unzensiert zu surfen, braucht man nur den Shadowsocks-Client und den zum Server passenden Schlüssel, der keinen Bezug zum Nutzer hat. Server lassen sich so konfigurieren, dass sie für alle Nutzer denselben Zugangsschlüssel verwenden. Unterm Strich können Betreiber selbst dann die Identität der Anwender nicht preisgeben, wenn ihr Server in fremde Hände fällt.

Mit Shadowsocks verbindet sich ein Client mit einem fernen SOCKS5-Proxy. Die Technik ähnelt dem Ansatz von SSH-Tunneln und wird auch bei Tor genutzt. Ist die Verbindung aufgebaut, leitet der Proxy den zu ihm gelangenden TCP- und UDP-Verkehr ins Internet.

Im Outline-Pelz

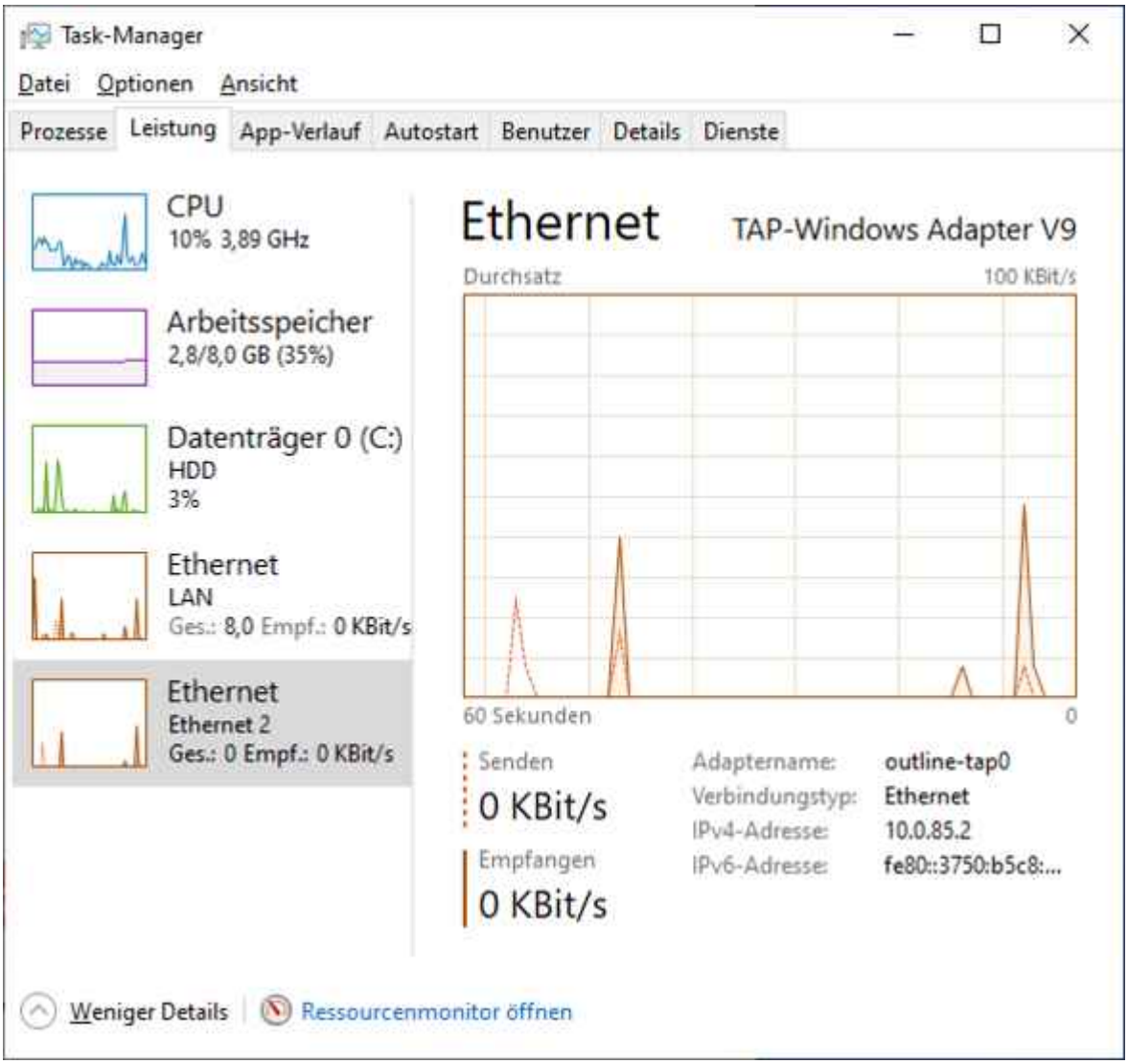
Die Jigsaw-Entwickler haben um Shadowsocks herum unter dem Namen Outline drei Anwendungen mit sehr übersichtlichen grafischen Oberflächen gebaut: Client, Server und Server-Manager. Alle drei sind für Linux, macOS und Windows erhältlich, die Clients auch für Android und iOS.



Von Googles Entwicklergruppe Jigsaw stammt auch die Shadowsocks-Variante Outline. Beide, Shadowsocks und Outline, verschleiern die Nutzdaten, um Firewallsperren zu entgehen.
Den Server installiert man mit dem Outline Manager typischerweise auf Cloud-Instanzen innerhalb von Minuten. Drei vereinfachte Installationen für DigitalOcean, Google und Amazon LightSail bietet der Manager gleich auf seiner Startseite an. Aber für das Einrichten auf anderen Linux-Servern oder im Firmennetz braucht man ebenso wenig Vorkenntnisse, denn die Installationsskripte erledigen den Großteil selbst.

Die Jigsaw-Entwickler bieten Outline hauptsächlich für Nachrichtenagenturen und Journalisten an, die aus Ländern mit Internet-Sperren berichten. Outline ist wie Shadowsocks quelloffen und gilt als sicher und vertrauenswürdig; es wurde 2017 und 2018 von Spezialisten auf Herz und Nieren geprüft. Allerdings lässt es sich einem Bericht zufolge trotz Verschleierungstechniken mit etwas Aufwand identifizieren (siehe ct.de/y9y1).

Deshalb lässt sich der Zugriff auf Outline-Server sperren. Das erfolgt allerdings per Hand und krude anhand von Ziel-IP-Adressen, weshalb sich Outline-Sperrungen nur dann häufen, wenn sich die politische Lage zuspitzt. Als Gegenmaßnahmen empfehlen die Outline-Entwickler den Betrieb mit mehreren IP-Adressen unter demselben Domainnamen (ct.de/y9y1).



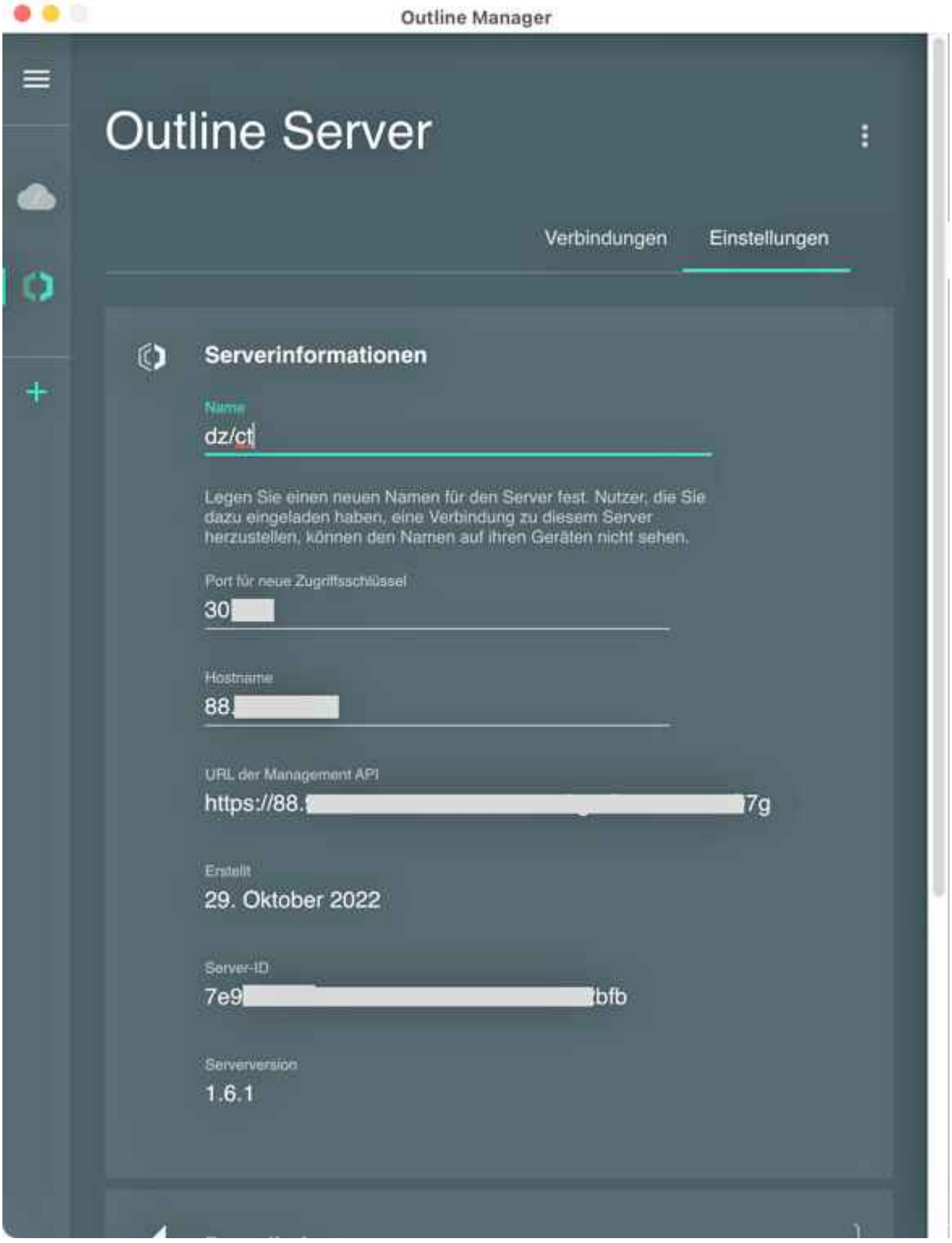
Der Outline-Client installiert auf Windows ein virtuelles TAP-

Interface und lenkt darüber allen ausgehenden Internet-Verkehr in den Tunnel zum Outline-Server.

Outline Manager und Server

Ausgehend vom Outline Manager haben wir den Outline-Server auf zwei Debian-VMs installiert, es klappte auf beiden im Nu und reibungslos. Dabei nimmt ein Bash-Skript dem Admin sehr vieles ab; es verlangt nur einige wenige Angaben. Am Ende fällt ein URL heraus, den man in den Outline-Manager kopiert und ein Zugangsschlüssel mitsamt Server-URL, die man an die Nutzer verteilt.

Darüber hinaus bietet der Manager nur wenige weitere Funktionen. Man kann für Clients Obergrenzen für das Übertragungsvolumen festlegen und Verwaltungsdaten wie IP-Adresse oder Server-ID ablesen – das wars auch schon. Infos und diverse Statistiken liefert das Monitoring-Tool Prometheus, das man auf dem Outline-Server über die lokale IP-Adresse 127.0.0.1 und die TCP-Ports 9090, 9091 und 9092 anzapft. Außerdem bietet Google einen Metrics-Server auf Grundlage der Google App Engine; er setzt Googles Cloud SDK voraus (ct.de/y9y1).



Das Einrichten des Outline-Servers startet man auf Linux, macOS oder Windows mit dem Outline Manager. Anschließend läuft auf dem Zielserver ein Bash-Skript und richtet dort einen Docker-Container mit Shadowsocks ein – was alles ohne besondere Netzwerkkenntnisse klappt.

Prinzipiell sollte der Server auch auf anderen Betriebssystemen laufen, denn er steckt in einem Docker-Container auf Basis der Alpine-Distribution 3.11.6 (siehe

Docker-Plattform Quay, ct.de/y9y1). Das Installationsskript des Outline Managers sieht aber nur Linux-Plattformen (x86_64) als Zielserver vor.

Um zu prüfen, was das Skript tut, lädt man es einfach aus dem GitHub-Projekt von Jigsaw (siehe ct.de/y9y1) auf einen PC und liest es in einem Editor. Unter anderem installiert es Docker, falls das fehlt, und richtet den Container mitsamt dem Zugriffsschlüssel ein.

Insgesamt liefen beide Server-Instanzen im mehrwöchigen Testbetrieb reibungslos. Zwar haben die Entwickler den Container seit zwei Jahren nicht aktualisiert, sodass die automatische Test-Routine von Quay viele und auch kritische Sicherheitslücken meldet. Sie betreffen aber nur den Befehl curl 7.67.0 (Release-Datum 6.11.2019), den man im Serverbetrieb nicht nutzt. Wer die Lücken trotzdem eliminieren will, findet die erforderlichen Update-Befehle im Quay-Repository (siehe ct.de/y9y1).

Outline Client

Der Outline Client ist ebenfalls flink installiert. Hat man ihm eine passende URL spendiert, baut er die Verbindung zum Server umgehend auf und signalisiert das im Menü. Fortan läuft jeglicher Internet-Verkehr durch den Tunnel. Auf Macs kann man das beispielsweise mit dem Befehl netstat -rn | grep 'default' auslesen. Dabei wird sichtbar: Der gesamte Verkehr wird an ein virtuelles TUN-Interface geleitet (z. B. utun10).

Mit ifconfig utun10 kann man die (lokale) Ziel-IP-Adresse auslesen (inet 169.254.19.0) und route -n get <domain> zeigt, über welchen Weg ein bestimmtes Ziel angesprochen wird:

route -n get ct.de

gibt zum Beispiel Folgendes aus:

route to: 193.99.144.80

```
destination: default
interface: utun10
```

Wer im Container herumspaziert, findet bald, dass die Jigsaw-Entwickler zur DNS-Auflösung der VPN-Clients die DNS-Resolver von Google konfiguriert haben. So schenkt man Google die Surf-Ziele der VPN-Nutzer. Google sichert immerhin zu, dass es DNS-Anfragen anonymisiert und spätestens nach 48 Stunden löscht. Wer trotzdem andere Resolver will, muss den Container editieren und etwa 9.9.9.9 eintragen (Resolver des gemeinnützigen Anbieters Quad9).

Fazit

VPN-Funktionen bilden heute für sehr viele Anwendungen die Kommunikationsgrundlage, obwohl die Technik ursprünglich nur zur Vernetzung von Standorten gedacht war. Manche Anwendungen verändern sich (Peer-to-Peer für Filesharing) und manche greifen Methoden aus teils scheinbar fernen Bereichen auf, etwa die Nutzdatenverschleierung bei Shadowsocks oder die RSA Blind Signatures beim Privatsphärenschutz von Apple und Google.

Das liegt in der Natur der Sache, denn die VPN-Entwicklung unterliegt einem starken Optimierungsdruck. Auf weitere Innovationen kann man ebenso gespannt sein wie darauf, ob und welche weiteren VPN-Anbieter diese aufgreifen. *(dz@ct.de)*

VPN-Infos: ct.de/y9y1

Pegasus bei BND und BKA

Pegasus bei BND und BKA

Nach und nach werden weitere Kunden der israelischen NSO Group bekannt. Offenbar haben auch deutsche Polizeibehörden und Nachrichtendienste die Spyware Pegasus gekauft.

Deutsche Behörden nutzen umstrittene Spyware

Nach und nach werden weitere Kunden der israelischen NSO Group bekannt. Offenbar haben auch deutsche Polizeibehörden und Nachrichtendienste die Spyware Pegasus gekauft.

Von Sylvester Tremmel

Das Bundeskriminalamt (BKA) und der Bundesnachrichtendienst

(BND) setzen offenbar die Überwachungssoftware Pegasus ein. Das berichten Zeit, Süddeutsche Zeitung, WDR und NDR. Im Fall des BKA soll das Bundesinnenministerium über den Einsatz informiert gewesen sein, nicht aber Innenminister Horst Seehofer selbst. Beim BND war angeblich das Bundeskanzleramt eingeweiht. Das Parlamentarische Kontrollgremium, dem unter anderem die Kontrolle des BND obliegt, soll nicht informiert worden sein.

Pegasus war im Juli dieses Jahres durch Veröffentlichungen des Rechercheverbundes „Pegasus Project“ der breiten Öffentlichkeit bekannt geworden. Den Recherchen zufolge wird Pegasus von einer Vielzahl von Akteuren auf der ganzen Welt eingesetzt; nicht nur zur Bekämpfung schwerwiegender Kriminalität, sondern auch, um Politiker, Oppositionelle, Menschenrechtsaktivisten und Journalisten zu überwachen.

Das steht im krassen Gegensatz zu den Versicherungen des israelischen Herstellers NSO Group: Das Unternehmen schreibt, man lizenziere seine Software nur an „ausgewählte, genehmigte, bestätigte und berechtigte Staaten und staatliche Behörden“. Pegasus dürfe nur zur „nationalen Sicherheit“ und in „größeren Ermittlungen“ von Sicherheitsbehörden zum Einsatz kommen. Andererseits betont die NSO Group auch, nicht zu wissen, wie ihre Kunden Pegasus tatsächlich nutzen.

Laut NSO Group kommt Pegasus nur gegen Terror und Kriminalität zum Einsatz.

Pegasus fürs BKA zu mächtig

Dem BKA wollte die NSO Group ihre Software 2017 verkaufen, berichtet Tagesschau.de. Dazu sei es nicht gekommen, weil das BKA Vorbehalte gehabt habe: Deutsches Recht unterscheidet zwischen Online-Durchsuchungen und der Quellen-Telekommunikationsüberwachung (Q-TKÜ). Im ersten Fall werden auf einem Gerät gespeicherte Daten ausgeleitet. Bei der Q-TKÜ wird dagegen nur die Kommunikation abgegriffen, analog zur abgehörten Telefonleitung. Pegasus habe diese Unterscheidung nicht getroffen und noch weitere Probleme aufgewiesen.

Nach einem Bericht der Wochenzeitung Die Zeit änderte sich dies 2020. Die NSO Group habe dem BKA eine angepasste Version von Pegasus zur Verfügung gestellt, die mit deutschem Recht vereinbar sein soll – zumindest nach Ansicht des BKA. Wie genau der BND Pegasus einsetzt, ist nicht bekannt.

Mit dem Einsatz von Pegasus stellen sich deutsche Behörden in eine Reihe von fragwürdigen Käufern, die erhebliche Zweifel daran aufkommen lässt, dass die NSO Group ihre Kunden ausreichend sorgfältig überprüft. Anfang Oktober befand etwa

ein englisches Gericht, dass Muhammad bin Raschid Al Maktum, Herrscher des Emirats Dubai, die Software eingesetzt habe, um seine Exfrau und ihre Anwälte zu überwachen.

Bedenklich ist auch der Verdacht, die NSO Group könnte Einblick in die mit Pegasus durchgeführten Überwachungsoperationen haben – entgegen ihrer Aussagen. Gegenüber der Zeit erklärten BND und BKA, das technisch ausschließen zu können. Die Zeitung berichtet aber von entgegenstehenden Aussagen ehemaliger Mitarbeiter der NSO Group. Demnach würden die exfiltrierten Daten über Server des Unternehmens fließen.

Hinzu kommt ein moralisches Problem: Um Software wie Pegasus auf Zielgeräte ausspielen zu können, muss die NSO Group schwerwiegende Sicherheitslücken in aktuellen Versionen von iOS und Android kennen und geheim halten. Die daraus erwachsende Gefährdung sämtlicher Smartphone-Besitzer wird in Kauf genommen. Kunden der NSO Group finanzieren dieses Geschäftsmodell, statt die breite Masse ihrer Bürger zu schützen.

Im Fall von Android ist nicht bekannt, über welche Lücken Pegasus auf Geräte gelangt. Unter iOS war ein Einfallstor mutmaßlich eine Lücke in der App iMessage. Darüber konnte Pegasus ausgespielt werden, ohne dass die iPhone-Nutzer irgendetwas tun mussten – eine sogenannte Zero-Click-Lücke. Die hat Apple mittlerweile geschlossen, welche weiteren Lücken die NSO Group noch kennt, weiß nur sie selbst. *(syt@ct.de)*

Recherchen zu Pegasus: ct.de/yfzj

ct.de/yfzj

- **The Pegasus Project** Seite des Pegasus Projekts beim Journalismus-Netzwerk Forbidden Stories.
- **Forensic Methodology Report: How to catch NSO Group's**

Pegasus Forensischer Bericht zu Pegasus des Security Labs von Amnesty International.

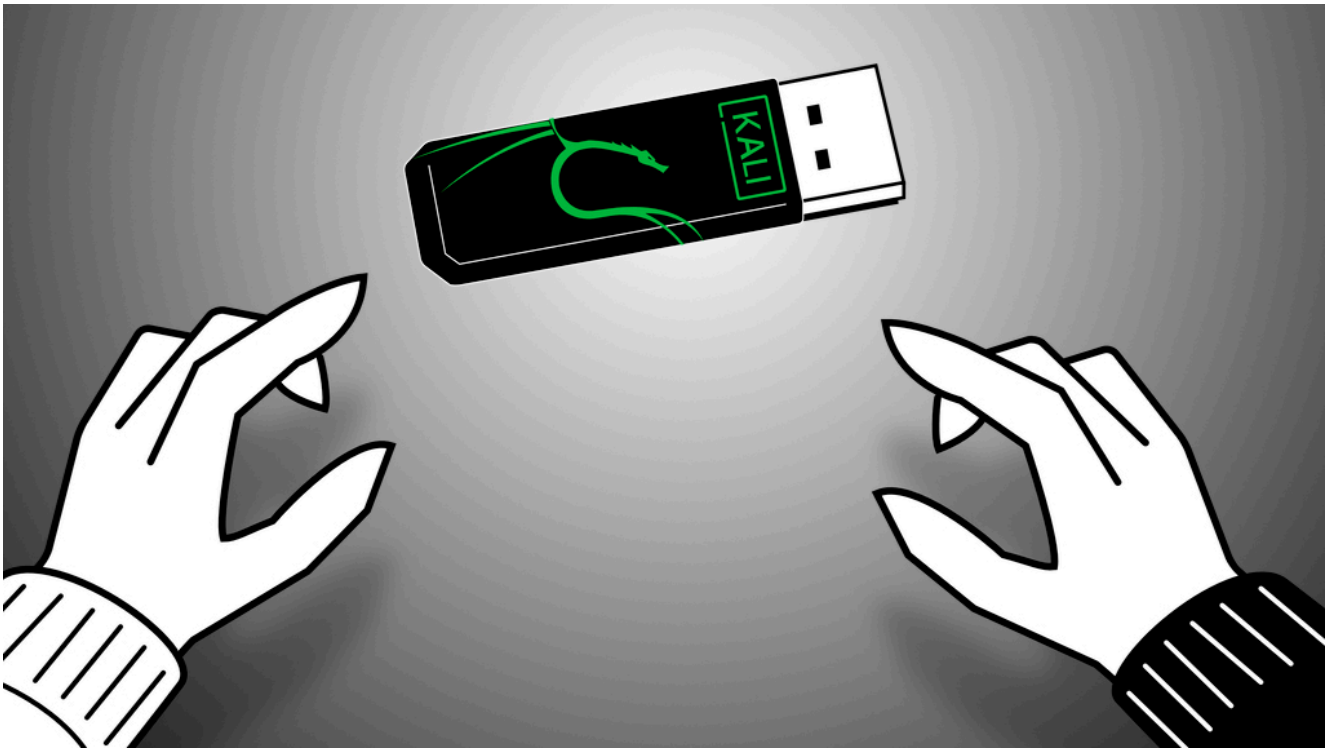
c’t-Berichterstattung zum Thema Pegasus

- **Infiziert ohne Klick: Amnesty International deckt Massenüberwachung durch Pegasus auf**
- **Rüffel vom Fachmann: Sicherheitsforscher fordert grundlegende iOS-Überarbeitung**
- **Spyware-Entdecker: Geheimdienst-Spionagetool Pegasus auf dem iPhone enttarnen**

Pegasus an deutschen Behörden

- **BKA bekam maßgeschneiderten Trojaner** Tagesschau.de zum Pegasus-Einsatz beim BKA.
- **Bundesnachrichtendienst setzt umstrittene Cyberwaffe ein** Zeit-Bericht zum Einsatz von Pegasus beim BND.
- **Bundesnachrichtendienst spitzelt mit Pegasus** Tagesschau.de zum Pegasus-Einsatz beim BND.

Kali Linux auf USB-Stick einrichten



Hacking-Stick

Mit Kali Linux können Sie etliche Hacking-Tools ohne Installation ausprobieren. Auf einem USB-Stick haben Sie es immer dabei.
Mit Kali Linux können Sie etliche Hacking-Tools ohne Installation ausprobieren. Auf einem USB-Stick haben Sie es immer dabei.

Von Ronald Eikenberg

Kali Linux ist in vielen Lebenslagen ein nützlicher Helfer: Es enthält etliche Hacking-Tools, die man sofort ausprobieren kann. Die oftmals umständliche Einrichtung der Programme fällt weg. Damit spüren Sie nicht nur Sicherheitsprobleme auf, die mitgelieferten Werkzeuge eignen sich auch zum Daten retten und für vieles mehr. Mit wenig Aufwand erstellen Sie sich einen bootfähigen USB-Stick, mit dem Sie sich selbst davon überzeugen können.

Als Grundlage dient ein Debian, das perfekt auf die Bedürfnisse der Hacking-Community zugeschnitten wurde. Deshalb ist Kali genauso wie einst sein Vorgänger BackTrack Linux seit

Jahren die erste Wahl bei Security-Experten und Hackern. Kali lässt sich wie jedes Betriebssystem installieren, doch das ist zum Ausprobieren gar nicht nötig. Im einfachsten Fall läuft das Hacker-Linux als Live-Betriebssystem vom USB-Stick – auf Wunsch auch mit Datenpartition, in der man dauerhaft Daten bunkern kann. Zudem gibt es allerhand virtuelle Maschinen sowie Images für Raspis und das mit Windows 10 eingeführte „Windows-Subsystem für Linux“ (WSL). Kurzum: Wer Kali testen möchte, der hat viele Optionen.

Kali-on-a-Stick

Dieser Artikel zeigt Ihnen das Einrichten eines Kali-Live-Sticks, den Sie universell einsetzen können, sowie die ersten Schritte, damit Sie komfortabel damit arbeiten können. Gegenüber einer virtuellen Maschine hat so ein Live-Stick den Vorteil, dass sein Betriebssystem direkt auf die Hardware des Rechners zugreifen kann. Das ist in Situationen wichtig, in denen ein hardwarenahes Hacking-Tool beispielsweise Direktzugriff auf Netzwerkkarte, USB-Geräte oder GPU benötigt.

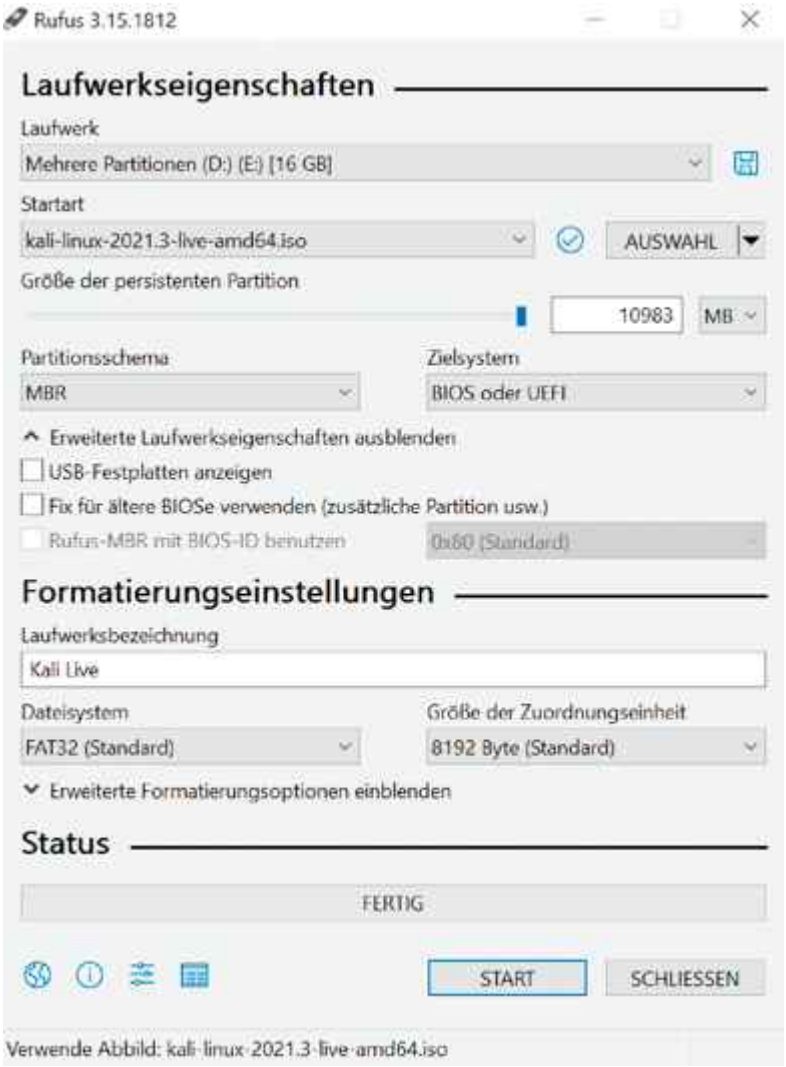
Auf der Download-Seite der „Live Boot“-Variante (siehe ct.de/ypk1) finden Sie zwei Kali-Versionen: Die stabile und getestete Snapshot-Version (etwa Kali 2021.3) und einen automatisch erstellten Weekly-Build, mit dem Sie näher am Puls der Zeit sind. Er enthält aktuellere Versionen der Komponenten, wodurch der erste Updatelauf schneller über die Bühne geht. Wenn Sie auf Nummer sicher gehen möchten, ist jedoch der Snapshot die bessere Wahl.

Live-Betriebssysteme sind üblicherweise vergesslich. Alle Änderungen am System landen lediglich im RAM und sind nach dem Herunterfahren verloren. Wenn Sie nicht jedes Mal bei Null anfangen möchten, können Sie eine Persistence-Partition anlegen, in der Kali sämtliche Änderungen speichert, einschließlich Einstellungen, Home-Verzeichnis und Updates. Nutzen Sie am besten einen modernen USB-3-Stick, da mit der Geschwindigkeit des Speichers auch die Performance des Live-

Systems steht und fällt. Ältere Stick-Semester bremsen das System unnötig aus und haben nicht selten Probleme beim Einsatz als Bootmedium. Moderne und flotte USB-Sticks bekommen Sie bei den bekannten Onlinehändlern bereits für weniger als 10 Euro. Der Stick sollte mindestens 8 GByte fassen.

Live-Linux mit Gedächtnis

Über das Anlegen der Persistence-Partition müssen Sie sich nicht den Kopf zerbrechen, denn das erledigen Sie beim Beschreiben des USB-Sticks nebenbei. Kali Linux erwartet eine ext3-Partition namens „persistence“, die sich über den gesamten überschüssigen Speicher Ihres Sticks erstrecken kann. Eine hohe Kapazität zahlt sich also aus. Bei einem 8-GByte-Stick kann sich der Speicherbereich für Ihre Daten immerhin bereits auf mehr als 3 GByte entfalten. Damit Kali die Partition erkennt, muss auf ihr eine Datei „persistence.conf“ mit dem Inhalt / union gespeichert sein.



Klick, Klick, Stick: Rufus erstellt nach ein paar Mausklicks einen bootfähigen Kali-Stick samt Persistence-Partition, in der Sie Daten dauerhaft ablegen können.
Sie könnten die Partition mit einem Partitionierer Ihrer Wahl (zum Beispiel GParted oder MiniTool Partition Wizard Free) von Hand anlegen, nachdem Sie den Stick mit dem Kali-Image bespielt haben. Doch warum kompliziert, wenn es auch einfach geht? Bei uns hat sich das Windows-Tool Rufus (siehe ct.de/ypk1) bewährt, das dem USB-Stick nicht nur das Kali-Image verpasst, sondern im gleichen Arbeitsgang auch eine geeignete Persistence-Partition.

Um einen Persistence-Stick mit Rufus zu erstellen, starten Sie das Tool und wählen ganz oben den angeschlossenen USB-Stick als Schreibziel aus. Anschließend speisen Sie über „Auswahl“ das Kali-ISO ein, zum Beispiel „kali-linux-2021.3-live-amd64.iso“. Achten Sie darauf, dass der Dateiname „live“

enthält, um sicherzustellen, dass Sie es mit der richtigen Datei zu tun haben – die „installer“-Versionen eignen sich ausschließlich zur Installation, sie enthalten keinen Livemodus.

Danach kümmern Sie sich um die Persistence-Partition. Ziehen Sie gleich darunter den Schieberegler „Größe der persistenten Partition“ ganz nach rechts, damit der Persistence-Bereich so groß wie möglich wird. Ändern Sie rechts daneben die Speichergrößeneinheit von „GB” auf „MB” und ziehen Sie den Schieberegler erneut nach rechts, um noch ein paar MByte extra herauszuquetschen. Den Rest können Sie auf den Vorgabewerten belassen. Klicken Sie auf „Start” und bestätigen Sie etwaige Rückfragen. Nach einigen Minuten, abhängig von der Schreibgeschwindigkeit Ihres USB-Sticks, ist Kali startklar.

Für Linux und macOS gibt es Rufus leider nicht, Sie können Ihr Glück mit UNetbootin versuchen (siehe ct.de/ypk1), das ähnlich funktioniert. Bei uns war es etwas wählerischer bei der Auswahl des Schreibziels, wir konnten aus ungeklärten Gründen nicht jeden USB-Stick damit bespielen. In vielen Fällen hat es jedoch erfolgreich einen bootfähigen Kali-Stick samt Persistence-Partition erzeugt. Wählen Sie unter „Abbild” einfach das Kali-ISO aus und in das Eingabefeld neben „Platz um Dateien zwischen Neustarts zu erhalten (nur Ubuntu)” tragen Sie irgendeine Zahl größer Null als Wunschgröße für die Datenpartition ein.

Die eingetippte Zahl wurde bei uns übrigens stets ignoriert, UNetbootin hat stattdessen die maximal mögliche Partitionsgröße genutzt. Abschließend starten Sie das Bespielen mit dem Ok-Knopf. Falls Sie den Stick lieber per Shell vorbereiten möchten, hilft Ihnen die offizielle Kali-Dokumentation weiter (siehe ct.de/ypk1). Dort erfahren Sie auch, wie Sie die Partition mit LUKS verschlüsseln, um sie vor unbefugten Zugriffen zu schützen.

Die Kali-Installation enthält etliche Security-Tools, die man ohne Installation ausprobieren kann.

Auf Probefahrt

Zeit für eine ersten Testfahrt! Wenn Sie ein aktuelles Windows nutzen, können Sie Ihren Rechner einfach über die erweiterten Startoptionen anweisen, vom Stick zu booten: Öffnen Sie über eine Startmenü-Suche „Optionen für den erweiterten Start ändern“ und klicken Sie unter „Erweiterter Start“ auf „Jetzt neu starten“. Nach dem Neustart wählen Sie die Option „Ein Gerät verwenden“ und anschließend den USB-Stick.

Es sollte der Grub-Bootmanager im Kali-Design erscheinen, der Ihnen diverse Startkonfigurationen anbietet. Wählen Sie „Live USB Persistence“, damit die Datenpartition des Sticks korrekt eingebunden wird. Falls Sie das nicht wünschen, wählen Sie mit dem obersten Eintrag den regulären Livemodus, der jedes Mal mit einem frischen System startet und nach der Nutzung sämtliche Änderungen vergisst.

Falls Sie den erweiterten Start nicht nutzen können, etwa weil Sie ein anderes Betriebssystem einsetzen, können Sie Ihren Rechner auch regulär vom Stick booten, indem Sie das System mit angeschlossenem Kali-Stick einschalten. Mit etwas Glück klappt der Start sofort, andernfalls müssen Sie im BIOS die Bootreihenfolge ändern oder, falls vorhanden, den Bootmanager des BIOS nutzen, um das System vom Stick zu starten.

Hierzu drücken Sie direkt nach dem Einschalten des Rechners eine bestimmte F-Taste. Welche genau, erfahren Sie in der Dokumentation des Herstellers oder über eine Google-Suche. Hier kocht jeder Hersteller sein eigenes Süppchen. Bei Asus beispielsweise öffnet sich das BIOS über die F2-Taste, mit F8 erreicht man die temporäre Auswahl des Bootmediums. Falls Sie den Rechner weiterhin nicht vom Stick starten können, probieren Sie am besten erst eine andere USB-Buchse, sonst einen anderen Stick aus.

Wenn Secure Boot in Ihrem Rechner aktiv ist, müssen Sie es zumindest vorübergehend im BIOS deaktivieren, da die Signaturüberprüfung an Kalis UEFI-Bootloader scheitert. Bei Surface-Geräten kann das Abschalten von Secure Boot dazu führen, das Sie später einmalig den Bitlocker-Wiederherstellungsschlüssel eingeben müssen, den Windows bei der Ersteinrichtung im Microsoft-Konto für Sie speichert.

Erste Schritte

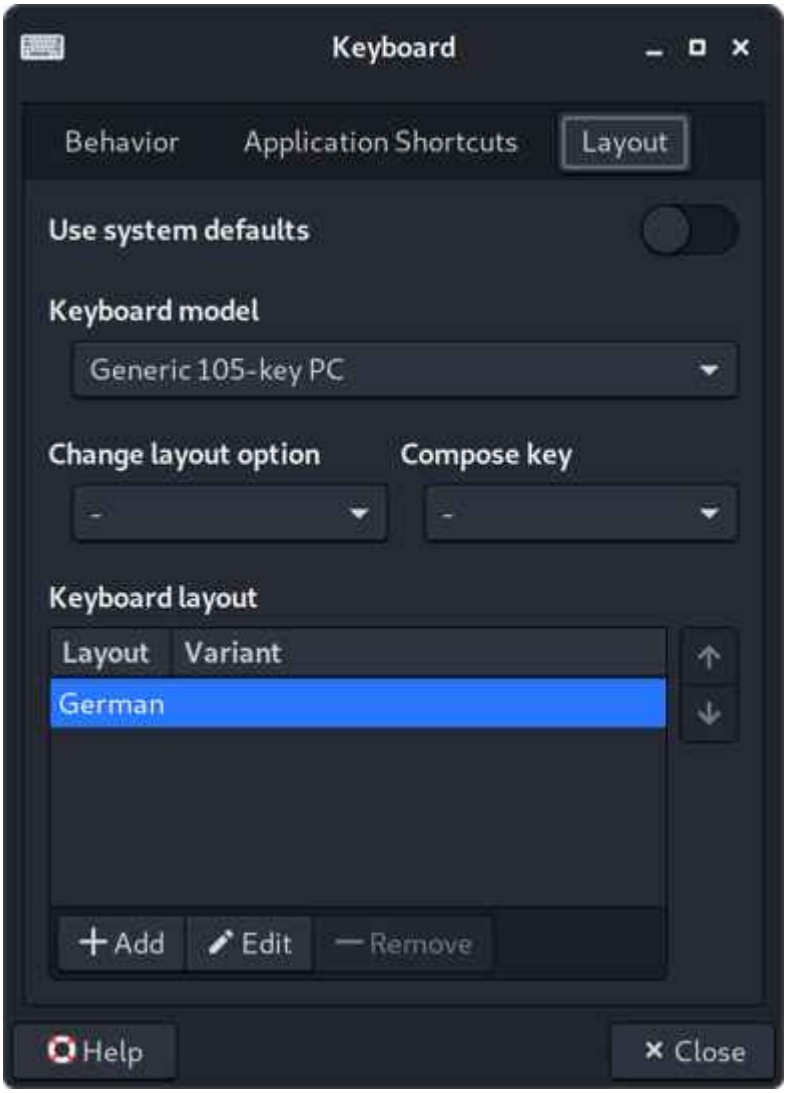
Hat alles geklappt, bootet Kali nach kurzer Zeit automatisch bis zum Desktop durch, die Eingabe eines Passworts ist nicht nötig. Falls sich Kali nach einiger Zeit der Inaktivität sperrt, erlangen Sie mit dem vorgegebenen Nutzernamen kali und dem gleichnamigen Passwort kali wieder Zugriff.

Die Xfce-Desktopumgebung macht Ihnen den Einstieg in die Kali-Welt leicht: Das Bedienkonzept unterscheidet sich nicht von anderen modernen Betriebssystemen. Ein wichtiger Dreh- und Angelpunkt ist das Kali-Menü, das Sie über das Logo oben links

und über die Windows-Taste erreichen. Hier finden Sie die Einstellungen und alle wichtigen Hacking-Tools, die bereits installiert sind. Die Kategorien wie „Password Attacks“ und „Wireless Attacks“ helfen Ihnen, sich zurechtzufinden und nützliche Werkzeuge zu entdecken.

Darunter befinden sich Klassiker wie Wireshark, Nmap, OWASP ZAP, Metasploit, aber auch exotischere Spezialtools, die nur für ganz bestimmte Aufgaben nützlich sind. Falls Sie schon wissen, wonach Sie suchen, können Sie einfach das Suchfeld ganz oben benutzen, um das gewünschte Tool aufzuspüren und zu starten. Eine Auswahl interessanter Hacking-Tools und Tipps zur Bedienung finden Sie auf Seite 24.

Nach dem ersten Start sind noch ein paar Handgriffe nötig, um komfortabel arbeiten zu können, denn das System läuft mit einer Standardkonfiguration und ist noch nicht an die hiesigen Bedürfnisse angepasst. So ist etwa das QWERTY-Tastaturlayout eingestellt, was unter anderem die Eingabe von Shell-Befehlen erschwert. Solche Einstellungen werden normalerweise während der Installation abgefragt, die Sie mit dem Livesystem gewissermaßen übersprungen haben. Doch das ist schnell korrigiert.



Erste Amtshandlung: Im Live-Modus sollte man zunächst das Tastaturlayout ändern.

Tastaturlayout ändern

Starten Sie die Tastatureinstellungen im Kali-Menü über „Settings/Keyboard“ und wechseln Sie auf den Registerreiter „Layout“. Deaktivieren Sie ganz oben den Schalter „Use system defaults“, um die darunterliegenden Einstellungen zu entsperren. Anschließend klicken Sie auf den „Add“-Button und wählen „German“ aus. Die Untervarianten hiervon können Sie ignorieren. Nach dem Hinzufügen können Sie „English“ über „Remove“ entfernen, da es nicht länger benötigt wird.

Falls Sie die Bedienoberfläche auf Deutsch umstellen möchten, öffnen Sie einfach den Terminal Emulator und tippen dort den folgenden Befehl ein: sudo localectl set-locale

LANG=de_DE.UTF-8. Sobald Sie sich über den Abmelden-Knopf in der rechten oberen Ecke des Bildschirms ausloggen („Log Out“) und wieder anmelden (mit kali/kali), spricht Kali Deutsch. Selbst die Tool-Kategorien im Kali-Menü sind übersetzt, was die ersten Schritte erleichtert. Wenn Sie mögen, ändern Sie jetzt noch das Anzeigeformat der Uhr oben rechts nach einem Rechtsklick übers Eigenschaften-Menü von 12 auf 24 Stunden. Rechts neben der Uhrzeit finden Sie das NetworkManager-Applet, über das Sie eine WLAN-Verbindung zum Router schaffen können – zum Beispiel für Updates. Dazu gleich mehr.

Falls Sie ein Notebook oder Display mit hoher Auflösung auf verhältnismäßig kleiner Fläche nutzen, zum Beispiel ein 15-Zoll-Notebook mit 4K-Display, dann wird Ihnen die dargestellte Kali-Bedienoberfläche möglicherweise winzig vorkommen. Mehr Bedienkomfort gibt es im HiDPI-Modus, der fast alles auf 200 Prozent skaliert, wie man es zum Beispiel von Windows kennt. Suchen Sie im Kali-Menü nach dem „Kali HiDPI Mode” und starten Sie ihn. Die Änderung ist sofort aktiv. Auf dem gleichen Weg können Sie auch den ursprünglichen Skalierungsmodus wiederherstellen. Auf grafische Anwendungen, die als root gestartet werden, hat der HiDPI-Modus derzeit leider keine Auswirkungen. Über das Menü „Anzeige“ können Sie die Darstellung weiter verfeinern, etwa durch Ändern der Auflösung oder individuelle Skalierungsstufen (dabei sind auch negative Werte erlaubt).

Die Shell ist Dein Freund

Auch wenn viele Tools eine grafische Oberfläche haben: Der Dreh- und Angelpunkt ist das Terminal. Mit Kali nutzen Sie die moderne Z-Shell (ZSH), mit der die Eingabe der Befehle so bequem wie möglich ist. Sie erfahren bereits beim Tippen, ob Sie auf dem richtigen Weg sind: Solange Ihre Eingabe rot gefärbt ist, würde die Ausführung zu einem Fehler führen. Bekannte Befehle erscheinen grün und mit der Tabulatortaste können Sie die aktuelle Eingabe von der Shell vervollständigen

lassen. So genügt es oft, die ersten Zeichen eines Kommandos einzugeben und Tab zu drücken. Genauso einfach hängen Sie Dateipfade an einen Befehl an, zum Beispiel, wenn Sie eine Datei mit Hashes in den Passwortknacker John the Ripper (siehe Seite 20) speisen möchten. Mit Strg+Alt+T öffnen Sie jederzeit ein neues Terminalfenster, Strg+Umschalt+T öffnet ein neues Tab in einem existierenden Terminal.

Wenn Sie Kali (oder seinen Vorfahren BackTrack) von früher kennen, wird Ihnen auffallen, dass Sie im System nicht länger als root mit uneingeschränkten Rechten unterwegs sind, sondern als „kali". Manche Tools benötigen jedoch weiterhin Superuser-Rechte, zum Beispiel bestimmte Betriebsmodi des Netzwerkscanners Nmap (siehe S. 25). Für solche Fälle starten Sie das Tool einfach mit einem vorangestellten sudo als root. Dies ist auch für viele Eingriffe ins System nötig, etwa zur Installation von Paketen und Updates. Hilfe zur Nutzung der Tools und Befehle erhalten Sie meist über man befehl oder, indem Sie -? oder --help an den Befehl anhängen.

Kali frischmachen

Mit den folgenden Befehlen bringen Sie Kali und die Tools auf den aktuellen Stand:

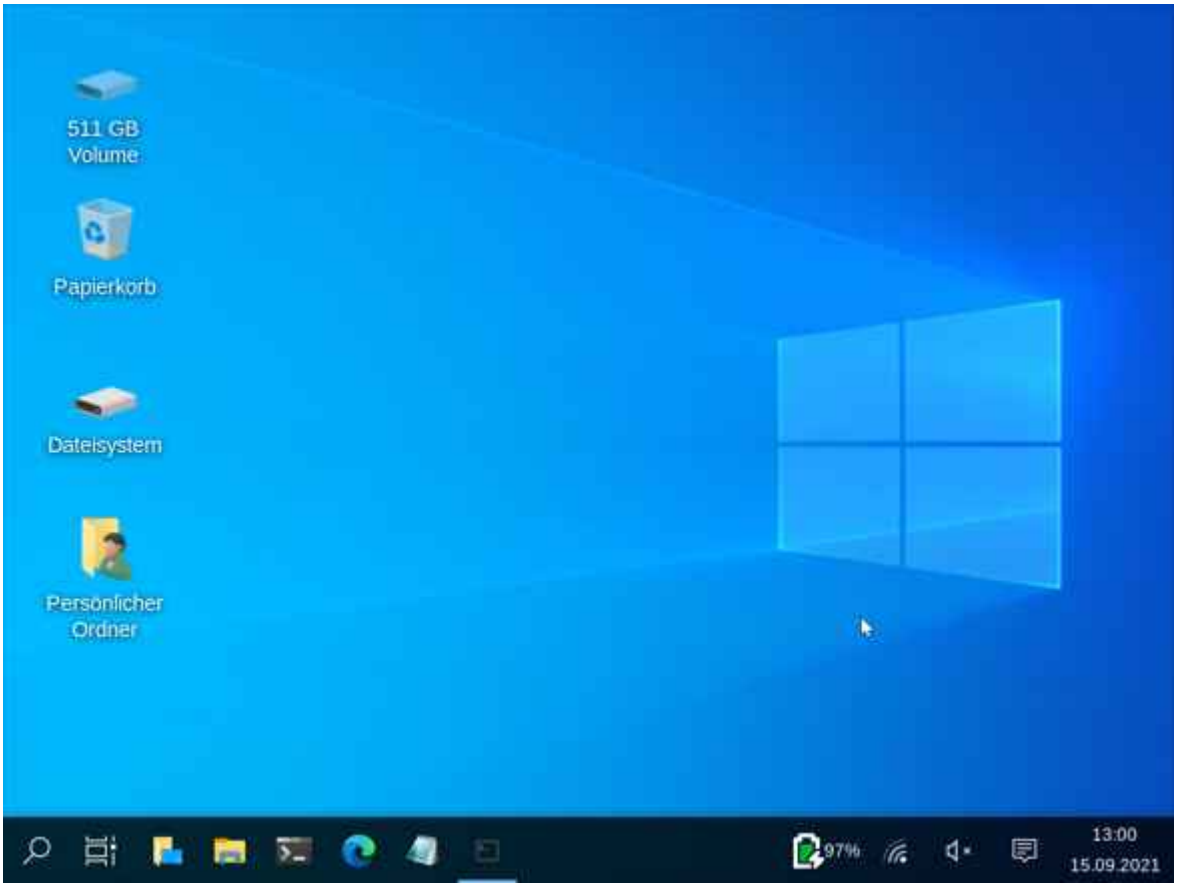
```
sudo apt update
sudo apt full-upgrade
```

Kali aktualisiert zunächst die Paketlisten und installiert anschließend die Updates. Je nachdem, wie aktuell Ihre Kali-Installation ist, kann dabei viel Zeit ins Land ziehen. Auch die Schreibgeschwindigkeit Ihres USB-Sticks spielt eine große Rolle. Möchten Sie ausschließen, dass der Upgrade-Vorgang zwischendurch darauf wartet, dass Sie Rückfragen beantworten, können Sie ein -y an den zweiten Befehl hängen, um alle Fragen im Vorfeld pauschal mit „Ja" zu bestätigen.

Tools nachrüsten

Falls Ihnen mal ein Tool fehlt, dann können Sie es wahrscheinlich aus dem Kali-Repository nachinstallieren. Sie können zum Beispiel nach Zenmap suchen, der grafischen Oberfläche für den Netzwerkscanner nmap: apt search zenmap

Danach installieren Sie den einzigen Suchtreffer zenmap-kbx mit sudo apt install zenmap-kbx. Das ist eines der ersten Tools, die als Kaboxer-Paket (Kali Applications Boxer) angeboten werden, was Sie an dem Namensbestandteil -kbx erkennen. Es handelt sich dabei um ein neues Containerformat, durch das sämtliche Abhängigkeiten in den passenden Versionen mitgeliefert werden können, ohne dass sie separat installiert werden müssen – ähnlich wie bei einem Docker-Container. Damit löst das Kali-Team das alte Problem, dass manche Tools aufgrund Ihrer Abhängigkeiten umständlich zu installieren sind oder sich mit anderen Tools in die Quere kommen. Ist der Vorgang abgeschlossen, können Sie das neue Tool über das Kali-Menü oder per Shell starten, in diesem Fall mit sudo zenmap-kbx.



Kali tarnt sich auf Wunsch als Windows 10.

Entdecke die Möglichkeiten

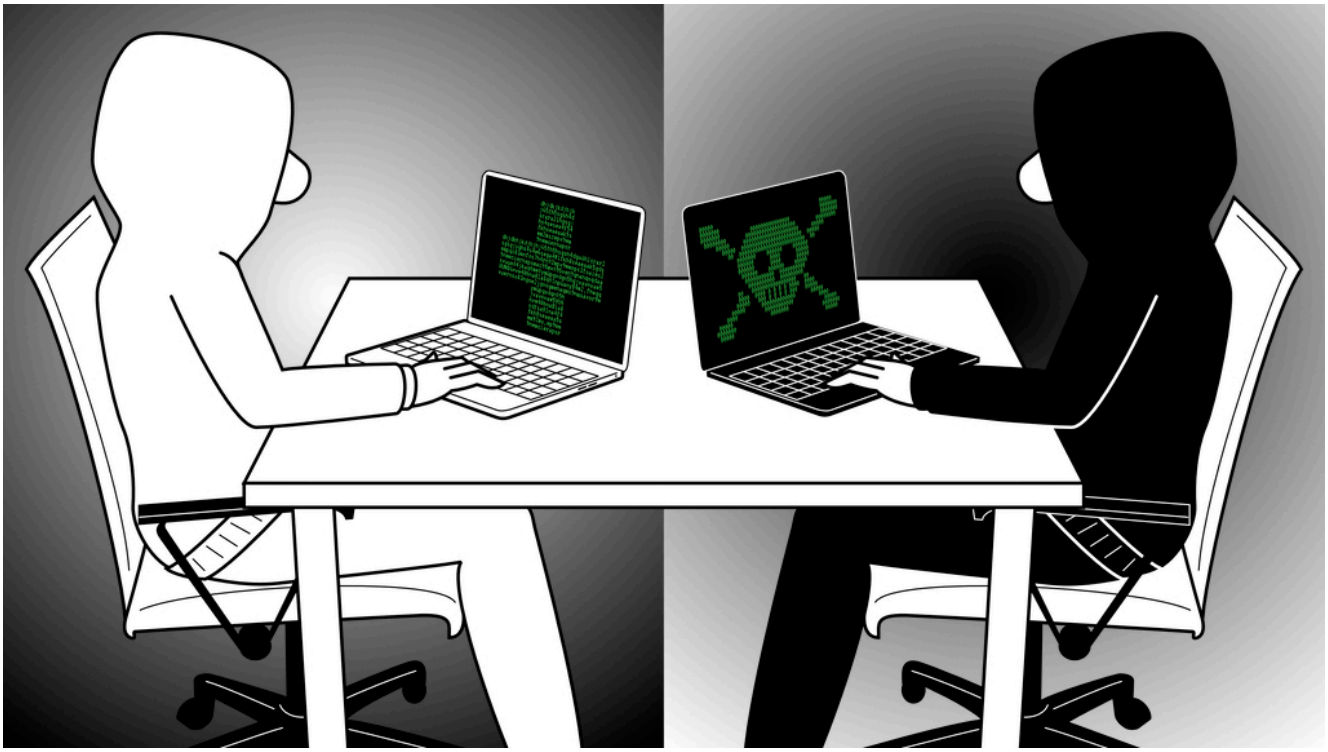
Mit Ihrem Kali-Stick steht Ihnen eine prall gefüllte Werkzeugtasche zur Verfügung, die Ihnen in vielen Situationen gute Dienste leistet. Die meisten Tools lassen sich zwar in die Oberkategorie „IT-Security“ einsortieren, doch Kali kann viel mehr. Wenn die Systemplatte streikt, können Sie mit TestDisk von Ihrem Stick einen Reparaturversuch starten und mit PhotoRec retten Sie verloren geglaubte Dateien. GParted ist ein leistungsfähiges grafisches Partitionierungsprogramm und Guymager erstellt Datenträgerabbilder, die sogar den Ansprüchen von Forensikern genügen. Falls Sie das Thema Forensik vertiefen möchten, sei Ihnen auch die Bootoption „forensic mode“ ans Herz gelegt: In diesem Betriebsmodus nimmt Kali keine Änderungen am System vor, was primär bedeutet, dass Laufwerke nie automatisch eingehängt werden. So kann man zum Beispiel ein Abbild der Festplatte ziehen, ohne Ihren Ist-Zustand zu verändern.

Zu guter Letzt sei noch der Undercover-Mode von Kali erwähnt, der mehr als eine Spielerei ist: Wenn Sie die Verknüpfung „Kali Undercover Mode“ über das Kali-Menü starten, verkleidet sich das Hacker-Linux kurz darauf als Windows 10. Die Taskleiste wandert Windows-typisch nach unten, als Hintergrundbild erscheint das blaue Windows-Bild. Das ist nicht nur witzig, es erlaubt Kali-Nutzern auch, im Alltag abzutauchen – und verhindert lästige Fragen neugieriger Mitmenschen.

Es gibt viel zu entdecken. Nehmen Sie sich etwas Zeit, um die zahllosen Möglichkeiten von Kali zu erkunden. Manchmal ist etwas Einarbeitung nötig, doch Sie erlernen wertvolles Hintergrundwissen darüber, wie die Dinge funktionieren und können fortan hinter die Kulissen blicken: Sorgt die neue Smart-Home-Kamera für mehr Sicherheit oder lässt sie auch Einbrecher in Ihr Wohnzimmer blicken? Wie lange hält Ihr WLAN einem Angriff stand? Ist Ihre WordPress-Installation ausreichend gegen Hacker geschützt? Mit Kali finden Sie es heraus. Inspiration liefert Ihnen der Artikel auf Seite 24, der viele wichtige und nützliche Tools detailliert vorstellt. (*rei@ct.de*)

Kali-Download & Tools: ct.de/ypk1

Hacking-Werkzeug für Fortgeschrittene



Gute Tools, böse Tools

Mit den Hacking-Tools von Penetrationtestern finden Sie Sicherheitslücken in Ihren Websites, Netzwerken und Anwendungen, bevor es andere tun.

Hacking-Werkzeug für Fortgeschrittene

Mit den Hacking-Tools von Penetrationtestern finden Sie Sicherheitslücken in Ihren Websites, Netzwerken und Anwendungen, bevor es andere tun.

Von Ronald Eikenberg und Alexander Königstein

Hollywood weiß Hacker-Aktivitäten in Szene zu setzen: Vor unzähligen Monitoren mit monochromatischen Benutzeroberflächen sitzen Gestalten im Kapuzenpulli und brechen durch die Firewalls. In der Realität geht es weitaus nüchterner zu, denn die eigentliche Action spielt sich hinter den Kulissen ab. Das ist aber nicht weniger faszinierend, denn Hacking-Tools

leisten erstaunliche Dinge, wenn man sie richtig einsetzt. Das setzt etwas Wissen und Erfahrung voraus, doch beides baut sich ganz von selbst auf, wenn Sie erst mal Feuer gefangen haben. In diesem Artikel stellen wir eine Auswahl interessanter Profi-Werkzeuge vor, die sowohl auf der dunklen als auch auf der hellen Seite der Macht genutzt werden. Stöbern Sie auch im Artikel „Hack Dich selbst“ auf Seite 18, der nützliche Problemlöser für den Alltag präsentiert.

Mit den im Folgenden vorgestellten Profi-Tools spüren Sie Sicherheitslücken in Ihren Websites, Netzwerken, Apps, IoT-Geräten und vielem mehr auf. Anschließend können Sie gezielt Schutzmaßnahmen ergreifen und die Schlupflöcher stopfen, bevor es zu spät ist. Die meisten Hacking-Tools laufen am besten oder ausschließlich unter dem Betriebssystem Linux. Eine gute Grundlage für die ersten Schritte ist **Kali Linux**, das von Haus aus bestens auf die Bedürfnisse von Hackern zugeschnitten ist. Auf Seite 30 erfahren Sie, wie Sie sich einen Kali-USB-Stick mit persistenter Datenpartition für Ihre Experimente erstellen. Download-Links und weiterführende Informationen zu allen vorgestellten Tools finden Sie online unter ct.de/ygg5. Aber genug der Vorrede – jetzt geht es in die Vollen!

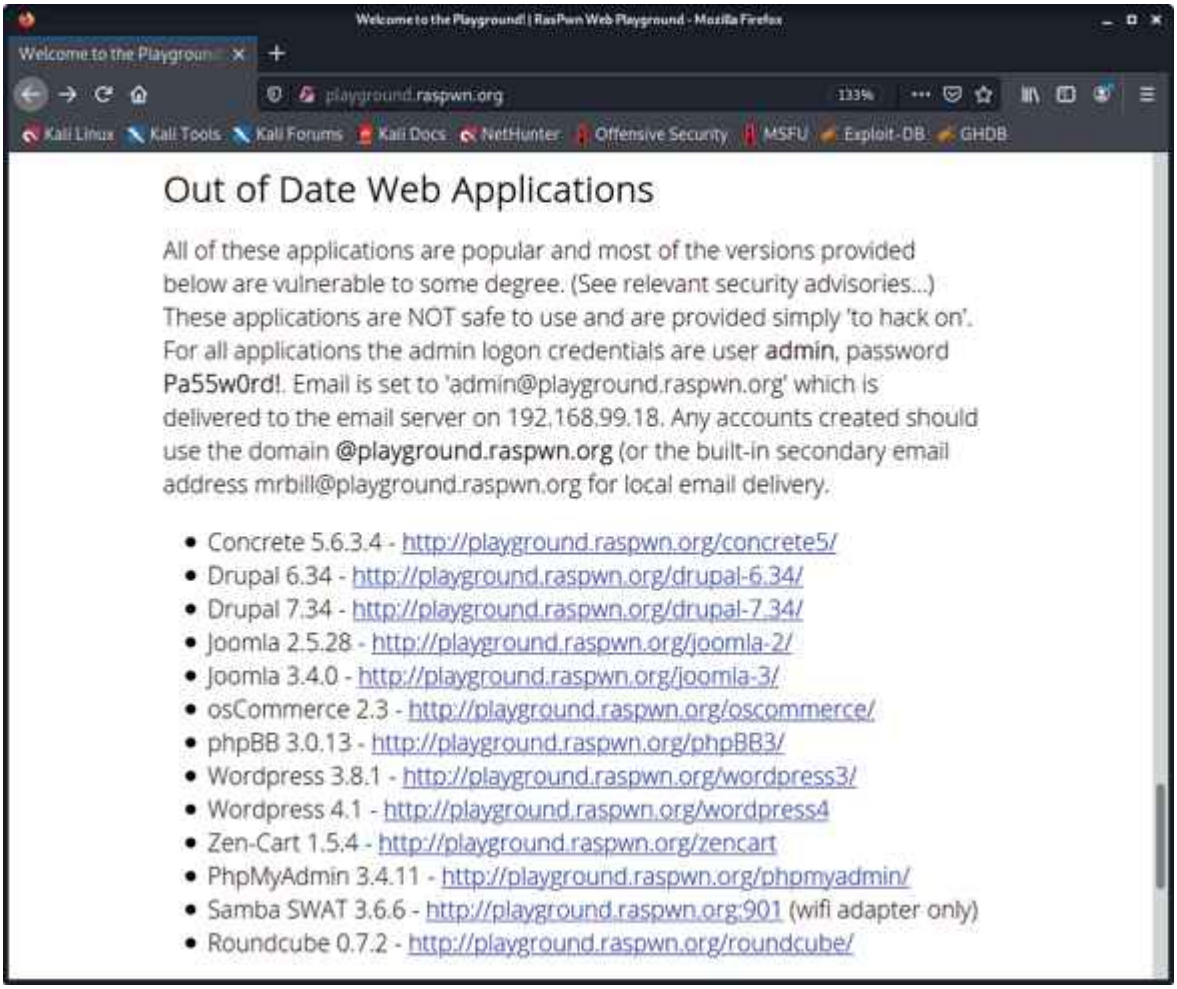
Angreifen erlaubt

Die hier genannten Hacking-Tools sind nicht illegal, aber natürlich dürfen Sie damit nicht gegen geltende Gesetze verstoßen (siehe Seite 170). Damit Sie gar nicht erst in Versuchung kommen, die Tools unerlaubt an fremden Servern zu testen, sollten Sie sich eine geeignete Übungsumgebung schaffen – zum Beispiel ein Testnetz, in dem sich ausschließlich Systeme befinden, die Sie attackieren möchten und dürfen.

Ein geeignetes Angriffsziel ist **RasPwn**, das ein ganzes Netzwerk voller verwundbarer Server simuliert, an denen Sie sich austoben können. Sie übertragen es einfach auf eine MicroSD-Karte, die Sie anschließend in einen Raspi-

Kleincomputer stecken (mindestens Raspi 2B). Nach dem Booten meldet sich ein WLAN namens „RasPwn OS“, zu dem Sie mit dem Passwort „In53cur3!“ eine Verbindung herstellen. Aus dem Netz öffnen Sie http://playground.raspwn.org mit einem Browser Ihrer Wahl, wo Sie mit allen wichtigen Informationen über das virtuelle Netzwerk und die angreifbaren Server versorgt werden. Ein Netzwerkkabel darf nicht mit dem Raspi verbunden sein, andernfalls hat das hochgradig verwundbare Image unter Umständen Zugriff auf Ihr Hauptnetzwerk und das Internet – was Sie tunlichst vermeiden sollten.

Zu den möglichen Angriffszielen zählen verwundbare WordPress-Installationen, eine steinalte Version des Webshop-Systems osCommerce, das Datenbank-Tool phpMyAdmin, ein Mailserver, Samba und so weiter. Auch das Debian-Linux, auf dem RasPwn basiert, hat schon fast sieben Jahre auf dem Buckel und ist so löchrig wie ein Schweizer Käse. Obendrauf gibt es zahlreiche Web-Applikationen wie OWASP Bricks und Damn Vulnerable Web Application (DVWA), die nur mit dem Ziel entwickelt wurden, möglichst verwundbar zu sein, um typische Sicherheitslücken am lebenden Objekt zu demonstrieren. Viele dieser Projekte sind online dokumentiert, wodurch sie sich hervorragend zum Lernen eignen (siehe ct.de/ygg5).



Das Raspi-Image RasPwn enthält etliche verwundbare Web-Apps – und das mit voller Absicht.

Netzwerk auskundschaften

Hat sich ein Angreifer Zugriff auf ein fremdes Netzwerk verschafft, etwa durch eine frei zugängliche Netzwerkbuchse im Aufenthaltsraum, eine per E-Mail eingeschleuste Malware oder ein schwaches WLAN-Passwort, dann wird er sich erst mal einen Überblick über die Geräte im Netz verschaffen, um mögliche Angriffsziele auszumachen. Hierbei ist der mächtige Netzwerkscanner **Nmap** (Network Mapper) die erste Wahl. Er spürt nicht nur die Rechner, Drucker, NAS, Server, Router und vieles mehr auf, sondern auch die darauf laufenden Dienste. Durch Skripte lässt sich der Scanner beliebig erweitern, etwa um die entdeckten Clients gleich noch auf Sicherheitslücken abzuklopfen. Das alles ist nützlich, um verwundbare Geräte im eigenen Netz aufzuspüren und sie anschließend entweder abzusichern oder aus dem Verkehr zu ziehen.

Nmap läuft auf Linux, macOS und Windows, bei Kali Linux ist er inklusive. Wenn Sie auf einer Shell nmap ohne Parameter eintippen, zeigt das Tool die wichtigsten Betriebsmodi an. Um einfach und schnell die offenen Ports eines bestimmten Hosts herauszufinden, hängen Sie einfach dessen IP-Adresse an den Befehl an, etwa nmap 192.168.178.1. Das müssen Sie zwar nicht als root ausführen, es lohnt sich aber: So finden Sie mehr über die Clients heraus, im konkreten Fall die MAC-Adressen. IPv6-Adressen scannen Sie mit dem Parameter -6.

Sie können den Scan auf einen IP-Bereich ausweiten, den Sie zum Beispiel mit 192.168.178.1-50 definieren (alle IP-Adressen, die mit 192.168.178 anfangen und mit .1 bis .50 enden). Oder Sie scannen gleich das gesamte /24-Subnetz (alle bis .255): nmap 192.168.178.0/24. Ist der Scan abgeschlossen, präsentiert Ihnen Nmap die Ergebnisse auf der Shell, vorher lässt das Tool nicht von sich hören. Wer ungeduldig ist, kann mit --stats-every 10s festlegen, dass Nmap regelmäßig ein Statusupdate ausgibt.

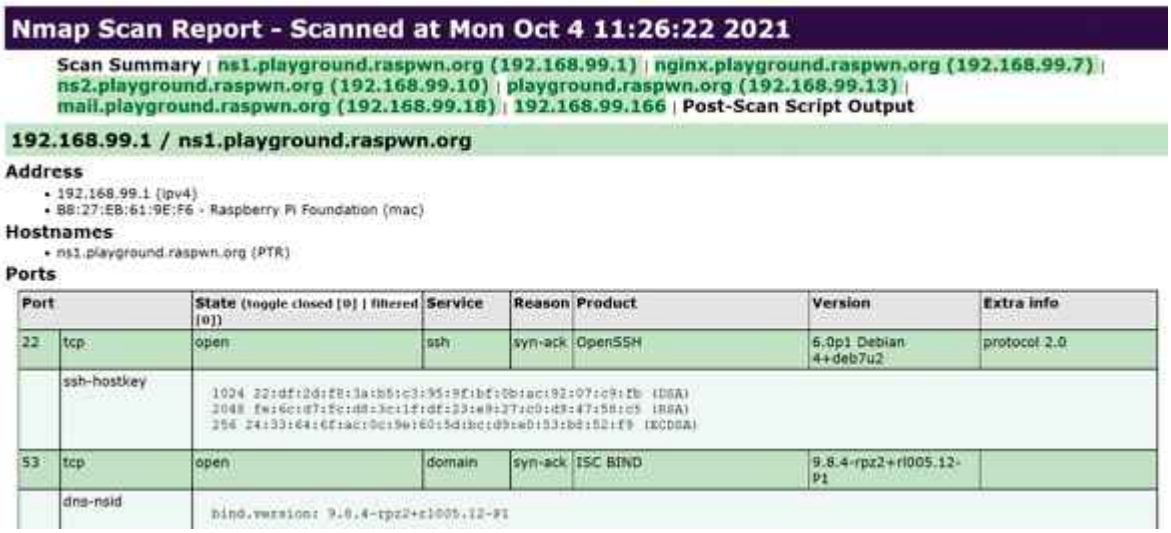
Wirklich komfortabel lesbar ist der Bericht auf der Shell nicht. Sie können jedoch leicht einen formatierten HTML-Report erstellen, indem Sie zunächst Nmap mit -oX ergebnis.xml anweisen, einen XML-Export der Ergebnisse zu schreiben. Anschließend bauen Sie daraus mit dem unter Kali vorinstallierten Tool xsltproc eine HTML-Datei, die Sie mit jedem Browser öffnen können: xsltproc ergebnis.xml -o ergebnis.html

Mit dem einfachen Scan kratzen Sie erst an der Oberfläche der Möglichkeiten. Mehr können Sie Nmap über verschiedene Scan-Optionen entlocken (siehe ct.de/ygg5). Sehr umfangreich ist der Modus -A, der unter anderem die Betriebssystem- und Versionserkennung (Fingerprinting) scharf schaltet. Diesen Modus sollten Sie mit sudo starten, damit Ihnen nichts entgeht. Aber aufgepasst: Nmap greift in diesem Fall aktiv auf die entdeckten Server zu, um Informationen einzuholen. Das kann zu unerwarteten Effekten führen, unser Epson-Drucker etwa

spuckt bei jedem Scan eine spärlich bedruckte Seite aus. Sie sollten Ihre ersten Schritte daher besser im oben erwähnten Testnetz machen.

Hardcore

Eine Übersicht über die mitgelieferten Skripte finden Sie in der Dokumentation von Nmap (siehe ct.de/ygg5). Praktisch ist etwa das vulners-Skript, das zu den ermittelten Serverversionen bekannte Schwachstellen aus einer Online-Datenbank heraussucht. Eigene Skripte können Sie in der Programmiersprache Lua entwickeln.

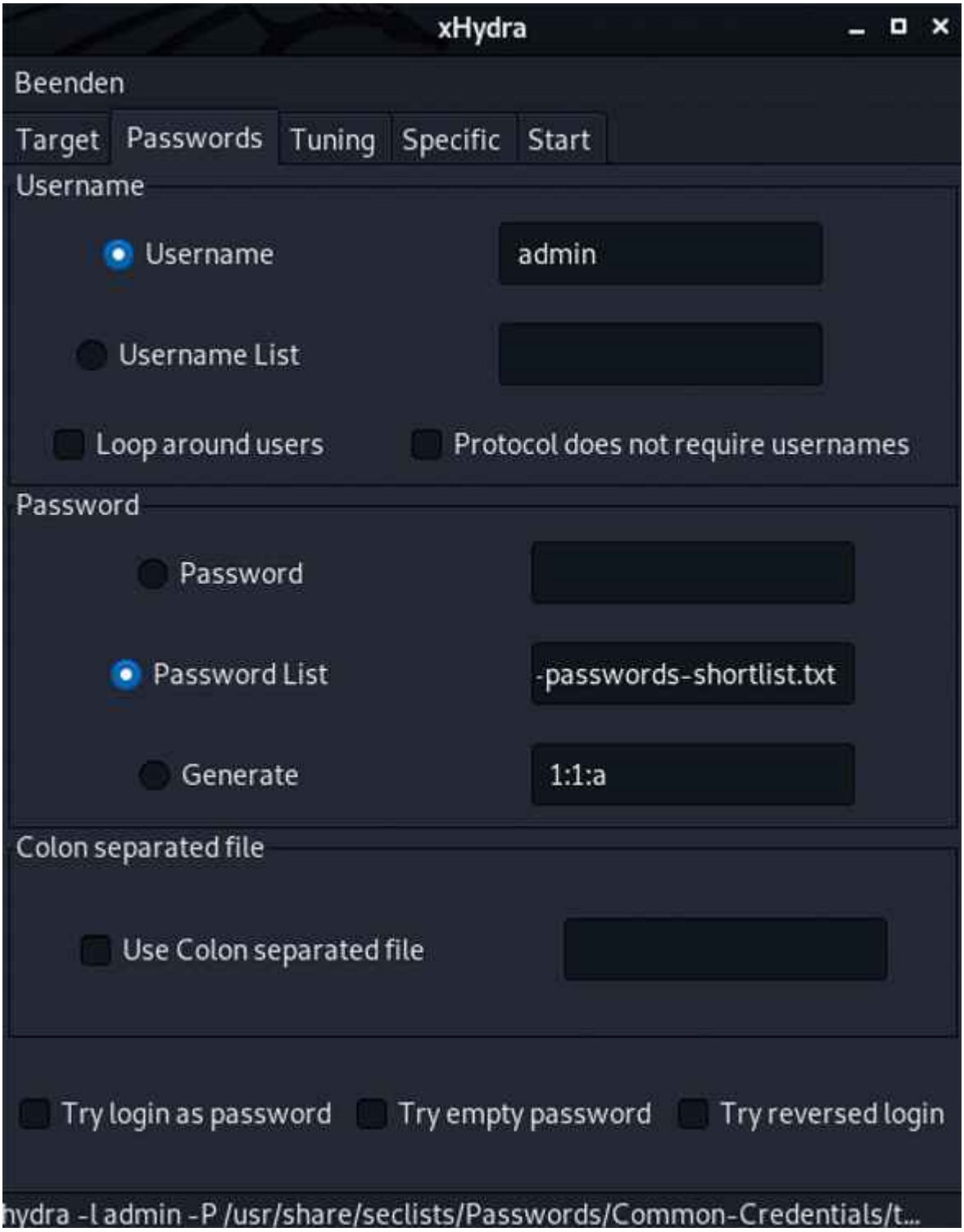


Was ist los im Netz? Der Netzwerkscanner Nmap liefert einen HTML-Bericht über alle Geräte und Dienste.

Zugriff auf Server

Vernetzte Geräte wie WLAN-Kameras oder Smart-Home-Komponenten sind oft für eine Überraschung gut: Auf manchen Exemplaren laufen unerwartete Dienste, die im Worst Case sogar mit einem Standardpasswort für Gott und die Welt aus dem Internet erreichbar sind. Die entdecken Sie zum Beispiel mit einem Nmap-Scan (siehe „Netzwerk auskundschaften“). Doch dann stehen Sie erst mal vor verschlossener Tür, denn das Zugriffspasswort ist häufig ebenso wenig dokumentiert wie der Dienst selbst. Solche Dienste sind ein unkalkulierbares Sicherheitsrisiko.

Fehlt Ihnen das Passwort, können Sie versuchen, es zu erraten – oder Sie überlassen dem Login-Cracker **Hydra** die ganze Arbeit. Er unterstützt viele gängige Protokolle wie FTP, HTTP(S), SMB, SSH, Telnet und VNC, wodurch er universell einsetzbar ist. Sie können Hydra wahlweise auf der Shell benutzen oder mit xHydra eine grafische Oberfläche starten, um ein paar Parameter einzustellen und die Passwortsuche zu starten. Wichtig sind das Ziel, der Port und das richtige Protokoll im ersten Tab. Danach folgt die Konfiguration des Nutzernamens und einer Passwortliste. Falls Sie gerade keine zur Hand haben, können Sie unter Kali das Paket seclists installieren, das diverse Listen unter /usr/share/seclists/Passwords ablegt. Im letzten Tab ist der Output des Tools zu sehen, also im besten Fall das gesuchte Passwort.



Sesam, öffne Dich: Hydra probiert, sich mit beliebig langen Passwortlisten bei einem Server einzuloggen.

IPv4-Traffic umleiten

ARP-Spoofing (auch ARP-Poisoning genannt) ist ein alter, aber nach wie vor effektiver Trick, um IPv4-Netzwerkverkehr umzulenken. Ein Angreifer im gleichen Netzwerk kann so den Datenverkehr anderer Teilnehmer ohne deren Zutun mitlesen und

manipulieren, etwa um sensible Daten abzugreifen oder Schadcode zu verbreiten. Das Ziel des Angriffs sind die ARP-Tabellen der Netzwerkclients. Darin ist vermerkt, unter welchen MAC-Adressen die IPs im lokalen Netz erreichbar sind. Durch gefälschte Nachrichten im Address Resolution Protocol (ARP) kann ein Angreifer die Tabellen verändern und Traffic umleiten, mitlesen und manipulieren. Eine solche Umleitung ist aber auch praktisch, um den Netzwerkverkehr einzelner Clients zu untersuchen, zum Beispiel, um herauszufinden, mit welchen Servern ein Smart-Home-Gerät spricht und ob die übertragenen Daten verschlüsselt sind.

Mit dem Sniffing-Tool **Ettercap** ist ARP-Spoofing sehr einfach, weil es alle nötigen Schritte vereint. Kali-Nutzer starten es über den Launcher („Sniffing & Spoofing/ettercap-graphical“). Wählen Sie zunächst das gewünschte Netzwerk-Interface. Anschließend müssen Sie noch die beiden IPs einstellen, zwischen denen Sie lauschen möchten, zum Beispiel Router-IP und die IP des Clients, für den Sie sich interessieren. Klicken Sie hierzu auf den Menüknopf (drei Punkte), „Targets“ und „Current Targets“. Über die Add-Buttons tragen Sie die IPs als Target 1 und 2 ein. Alternativ können Sie auch erst mal im lokalen Netz nach Clients scannen. Klicken Sie dafür im Menü unter „Hosts“ auf „Scan for hosts“. Kurz darauf können Sie die Netzwerkteilnehmer unter „Hosts/Host list“ einsehen und per Rechtsklick als Target hinzufügen.

Verkehrsumleitung: Ettercap nutzt ARP-Spoofing, um den Datenverkehr anderer Rechner über sich umzuleiten.
Jetzt müssen Sie das ARP-Spoofing nur noch auslösen: Klicken Sie oben rechts auf den Knopf, der an eine Weltkugel erinnert („MITM menu“) und auf „Arp poisoning…“. Über das Menü und „View/Connections“ können Sie live beobachten, wie die Daten durch Ihr System fließen. Sie erfahren dort unter anderem IP-Adresse, Hostname und Land der Gegenstelle, den genutzten Port und den Datenumfang. Ein Doppelklick auf eine Verbindung zeigt die übertragenen Daten an. Interessant sind zum Beispiel unverschlüsselte HTTP-Verbindungen auf Port 80, weil Sie deren Inhalt ohne weitere Hilfsmittel als Klartext lesen können.

Ettercap bringt einige interessante Plug-ins mit, die Sie im Menü unter „Plugins/Manage plugins“ durchstöbern und per Doppelklick aktivieren können. Darunter findet sich auch ein Gegengift für ARP-Spoofing: Der „arp_cop“ soll ARP-Manipulationen anzeigen. Wenn Ihnen die Analysefunktionen von Ettercap nicht ausreichen, können Sie Werkzeuge wie Wireshark nutzen, denn der angezapfte Traffic ist auf dem anfangs eingestellten Netzwerk-Interface sichtbar. Mit den Linux-Werkzeugen iptables oder nftables können Sie den Datenverkehr

zudem beliebig umleiten, zum Beispiel an einen lokalen Server.

WLAN auf dem Prüfstand

Funknetzwerke müssen viel aushalten, denn jeder in Reichweite kann sie attackieren. Wenn Sie sich nicht darauf verlassen möchten, dass Ihr WLAN schon sicher genug sein wird, können Sie mit Hacking-Tools die Probe aufs Exempel machen. Kali hat mehrere davon an Bord, die unterschiedliche Angriffsszenarien durchspielen. Zur Nutzung benötigen Sie ein WLAN-Interface, das sich in den „Monitor Mode“ schalten lässt und zudem gut von Linux unterstützt wird. Solche gibt es als USB-WLAN-Adapter schon für weniger als 20 Euro, zum Beispiel von CSL Computer (Modell 27395) oder Alfa Network. Ob Ihr Interface den nötigen Modus unterstützt, erfahren Sie über eine Google-Suche nach dem Chipsatz, etwa „Ralink RT5572 monitor mode“.

Um die gängigsten Angriffsarten zu simulieren, können Sie zu **wifite2** greifen, das diverse WLAN-Hacking-Werkzeuge für Sie ansteuert, um Sicherheitsprobleme aufzuspüren. Sie starten es wie folgt:

```
sudo wifite --random-mac --kill
```

Die Option --random-mac sorgt dafür, dass die genutzte Geräteadresse des WLAN-Adapters zufällig ausgewürfelt wird und --kill beendet störende Prozesse, die dem Tool in die Quere kommen könnten. Wifite fragt Sie zunächst, welches WLAN-Interface genutzt werden soll und macht sich anschließend sofort an die Arbeit. Kurz darauf listet es alle Netze in Reichweite auf.

Mit wifite2 finden Sie heraus, wie sicher Ihr WLAN wirklich ist. Im ersten Schritt zeigt es alle Netze in Reichweite samt Verschlüsselung und WPS-Status an.
Sobald Sie Ihr WLAN gefunden haben, beenden Sie den Scan mit Strg+C und geben die Indexzahl des Netzes ein. Wifite testet anschließend die wichtigsten Angriffsmöglichkeiten der Reihe nach durch, allen voran WPS-Attacken (Pixie Dust und Brute Force auf die PIN), die bei anfälligen Routern am schnellsten zum Ziel führen. Danach nimmt sich das Tool WPA(2) zur Brust und schließlich das steinalte WEP-Verfahren. Gegen WPA3 kommt es derzeit nicht an.

Der WPA(2)-Angriff läuf relativ simpel ab: Zunächst zwingt wifite die Clients per Deauthentication-Paket, die Verbindung zum Router zu trennen. Bei der anschließenden Neuanmeldung zeichnet es den Handshake auf und setzt anschließend den Passwort-Cracker hashcat darauf an. Der probiert eine Reihe von Passwörtern aus einer langen Liste durch, bis er fündig wird. Die wichtigsten Schutzmaßnahmen in aller Kürze: Nutzen Sie lange WPA-Passwörter (mindestens 16 Zeichen, besser mehr), aktivieren Sie möglichst WPA2/3 (Mixed Mode) und die geschützte Anmeldung von WLAN-Geräten (Protected Management Frames, PMF).

Datenlecks im Webserver finden

Webserver sind prinzipbedingt meist für jeden erreichbar – und damit zwangsläufig auch für Angreifer, die nach Sicherheitslücken, Datenlecks und schwachen Passwörtern suchen. Das geschieht längst nicht mehr mühsam von Hand, sondern automatisiert. So können die bösen Buben tausende Websites innerhalb kurzer Zeit auf Schwachstellen abklopfen und müssen bei der Wahl ihres Angriffsziels nicht wählerisch sein.

Wenn Sie eine Website betreiben, müssen Sie also fest mit ungebetenem Besuch rechnen. Und wenn es eine Sicherheitslücke gibt, wird diese früher oder später auch ausgenutzt. Sie können den Angreifern jedoch die Petersilie verhageln, indem Sie sich deren Tools zu eigen machen, um etwaige Schwachstellen selbst frühzeitig zu finden. Auch diese Tools dürfen Sie nur gegen eigene Server und niemals unbefugt gegen fremde Systeme einsetzen, sonst drohen juristische Konsequenzen (siehe Seite 170). Beachten Sie, dass die Werkzeuge sehr viele Anfragen und damit potenziell auch eine hohe Last erzeugen, was die Erreichbarkeit des Servers beeinträchtigen kann.

Ein einfaches, aber effektives Werkzeug zur Suche nach Datenlecks ist **DIRB**. Es probiert eine lange Liste mit gängigen Verzeichnisnamen wie /admin, /backups oder /internal durch, um Ordner zu finden, die nicht für die Öffentlichkeit bestimmt, aber trotzdem für jeden zugänglich sind. Ferner kann das Hacking-Programm Verzeichnisnamen per Brute Force erraten. Gibt es einen Treffer, versucht DIRB auch noch mögliche Unterordner zu entdecken. Die Bedienung ist einfach:

```
dirb https://ihre-website.example
```

Unzureichend geschützte Verzeichnisse sind häufig die Ursache für Datenlecks, etwa wenn darin Backups der MySQL-Datenbank oder Konfigurationsdateien mit Zugangsdaten gespeichert sind.

Diese Blindgänger sollten Sie rechtzeitig entschärfen, zum Beispiel durch einen Zugriffsschutz auf dem Verzeichnis, sofern die Daten überhaupt auf dem öffentlichen Server liegen müssen.

WordPress-Lücken aufspüren

Das Content-Management-System WordPress ist sehr verbreitet (siehe S. 60 ff.) und bei Angreifern entsprechend hoch im Kurs. Häufig wird es in veralteten – und somit verwundbaren – Versionen betrieben oder mit anfälligen Plug-ins und Themes. Auch Konfigurationsfehler begünstigen eine Fremdübernahme. Solche Schlupflöcher aufzudecken ist inzwischen ein Kinderspiel – zum Beispiel mit dem WordPress Security Scanner **WPScan**. Der kann Ihnen gute Dienste beim Absichern Ihrer Website leisten.

Auf der GitHub-Seite des Ruby-Tools erfahren Sie, wie Sie es unter Linux, macOS und als Docker-Container an den Start bringen (siehe ct.de/ygg5). Kali-Nutzer können sich das sparen, das Programm ist vorinstalliert. Um Ihre WordPress-Installation zu scannen, füttern Sie WPScan einfach mit der URL: wpscan --url https://ihre-website.example/wordpress

Bevor die Analyse beginnt, lädt der Security Scanner eine Datenbank mit aktuellen Infos aus dem Netz. Das geschieht normalerweise automatisch, wenn Sie es jedoch auf die verwundbaren WordPress-Installationen von RasPwn loslassen möchten (siehe „Angreifen erlaubt“), haben Sie keine Internetverbindung, solange Sie mit dem Raspi-Testnetz verbunden sind. In diesem Fall sollten Sie sich zunächst mit Ihrem normalen Netz verbinden und das Update mit wpscan --update manuell starten. Trennen Sie die Verbindung danach, ehe Sie schließlich den Scan aus dem RasPwn-Netz anwerfen.

Nach und nach gibt WPScan interessante Informationen über die WordPress-Installation aus, darunter die WordPress-Version samt Erscheinungsdatum und eine Einschätzung, ob diese Ausgabe

nach aktuellem Stand der Dinge sicher ist. Weiterhin identifiziert das Tool die Versionen von Webserver und PHP sowie Themes, Plug-ins und diverse Konfigurationsfehler. Prinzipiell kann man selbst im Netz recherchieren, welche Sicherheitslücken in den identifizierten Versionen klaffen. Aber auch das kann Ihnen WPScan abnehmen. Diese Informationen fragt das Tool über ein Web-API vom Server der Entwickler ab – dafür ist eine kostenfreie Registrierung nötig (siehe ct.de/ygg5).

Datenbank-Lecks verhindern

Die Kronjuwelen einer Website sind häufig Kunden- oder gar Nutzerdaten. Diese können Onlinegauner im Darknet leicht zu Geld machen. In der Regel bewahren Webanwendungen solche Daten in einer Datenbank auf, die natürlich gut geschützt sein sollte. Die Betonung liegt auf sollte, denn allzu oft gelingt es Cyberkriminellen, Kundendaten im großen Stil aus Datenbanken abzugreifen.

Eine häufige Ursache sind sogenannte SQL-Injection-Lücken: Dabei spricht der Angreifer nicht direkt mit dem Datenbankserver, sondern versucht stattdessen, die Webanwendung dazu zu bringen, eingeschleuste SQL-Befehle auf der Datenbank auszuführen. Das Resultat ist häufig, dass die Datenbank über die Web-Anwendung massenweise sensible Datensätze ausspuckt.

Sie ahnen es vielleicht schon: Auch für solche Lücken gibt es ein Hacking-Tool, in diesem Fall **SQLmap**. Es unterstützt zahlreiche Datenbanken, unter anderem Oracle, MySQL, MariaDB, MS SQL Server, PostgreSQL und SQLite. Je nach Datenbanktyp und Berechtigungen kann es auch Dateien auf den Webserver schreiben. Hacker können so versuchen, eine Web-Shell hochzuladen, um den Server dauerhaft fernzusteuern.

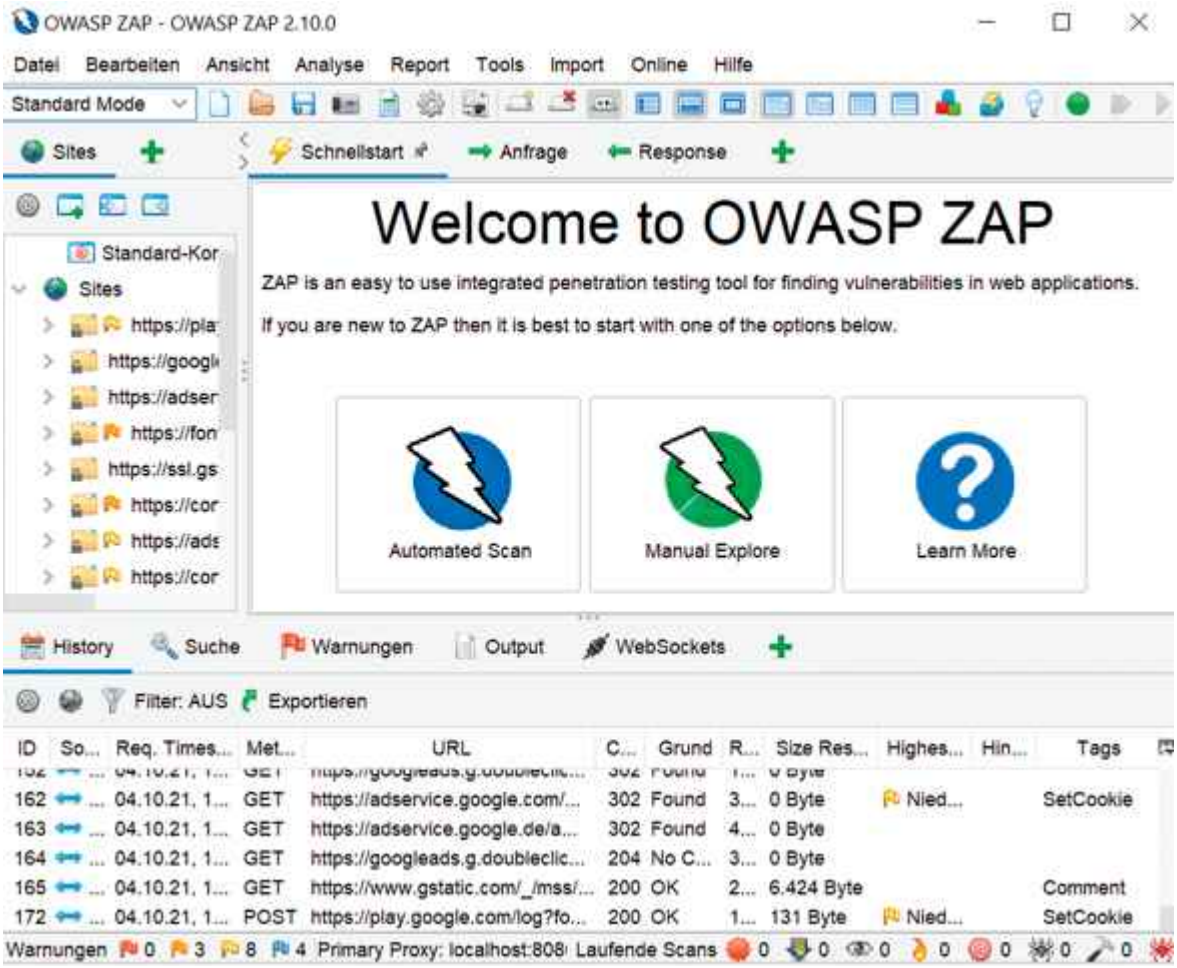
Für einen ersten Funktionstest können Sie die absichtlich anfällige „Wacko Picko“-Website von RasPwn mit SQLmap scannen.

Das Login-Formular der Website sendet beim Abschicken zwei POST-Parameter, nämlich „username“ und „password“, die der Schwachstellenscanner in diesem Beispiel in die Mangel nehmen soll. Um zu überprüfen, ob die Website bei der Auswertung dieser Parameter patzt, können Sie das Tool mit --data anweisen, genau das herauszufinden:

```
sqlmap -u "http://wackopicko.playground.raspwn.org/users/login.php" --data="username=1&password=1" --banner
```

Die Option „banner“ findet die Datenbankversion und das Betriebssystem des Servers heraus, wenn die Website verwundbar ist. Falls Sie den Datenbankinhalt gleich auslesen möchten, ersetzen Sie --banner einfach durch --dump.

Solche SQL-Injections vermeiden Sie, indem Sie Eingaben von außen konsequent überprüfen, bevor sie verarbeitet oder gar in Datenbankbefehle integriert werden. Weiterhin ist der Einsatz sogenannter „Prepared Statements“ sinnvoll, bei denen Sie zunächst den Aufbau des SQL-Befehls festlegen, ehe Sie darin einen Platzhalter mit den von außen angelieferten Werten füllen. Am besten basteln Sie die Datenbankbefehle nicht selbst zusammen, sondern setzen auf eine hinreichend getestete ORM-Bibliothek (Object-Relational Mapping), die bereits gegen alle Eventualitäten abgesichert ist.



Der Zed Attack Proxy (ZAP) macht verschlüsselten Datenverkehr im Klartext sichtbar und spürt Schwachstellen in Web-Anwendungen und APIs auf.

Browser- und App-Traffic

Der **OWAP Zed Attack Proxy (ZAP)** ist ein universelles Werkzeug zur Analyse und Manipulation von Web-Traffic (HTTP/HTTPS). Sie können sich damit zum Beispiel zwischen Browser und Internet klemmen oder den Datenverkehr Ihres Smartphones durch den Proxy schleusen, um herauszufinden, welche Daten wohin übertragen werden. Eine Stärke des ZAP ist, dass es die identifizierten Gegenstellen, also Webanwendungen, API-Endpunkte und so weiter gleich noch auf Sicherheitsprobleme abklopfen kann. ZAP ist eine Java-Anwendung und läuft unter Windows, Linux und macOS.

Nach dem ersten Start klicken Sie am besten auf den Browser-Knopf in der Symbolleiste, um einen perfekt vorkonfigurierten

Webbrowser zu starten. Dessen Datenverkehr wird automatisch durch den Proxy geschleust. Öffnen Sie damit eine Website, um den Traffic in ZAP zu inspizieren. Wenn Sie den Browser auf diese Weise starten, schleust ZAP in die geöffneten Websites eine eigene Oberfläche namens ZAP HUD ein, über die Sie zahlreiche Funktionen direkt aus dem Browser steuern können. Klicken Sie auf den Knopf „Take the HUD Tutorial“, um eine Einführung zu erhalten und einige der nützlichen Funktionen kennenzulernen.

Gemischtwaren

Dieser Artikel liefert Ihnen nur eine kleine Auswahl an Hacking-Tools. Das Angebot ist riesig und täglich kommen neue dazu. Einige davon sind sehr komplex oder nur für bestimmte Zielgruppen interessant. Dazu zählt das modular aufgebaute Pentesting-Framework **Metasploit**, das professionelle Penetrationtester nutzen, um einen kompletten Angriff zu simulieren: vom Aufspüren der Ziele über das Ausnutzen von Sicherheitslücken bis hin zum Ausleiten der Datenbeute. Falls Sie sich eingehender mit Hacking beschäftigen möchten, sollten Sie einen Blick darauf werfen. In eine ähnliche Kerbe schlägt **PowerShell Empire**, das Pentestern weitreichenden Rechnerzugriff verschafft, ohne verdächtigen Binärcode auf dem System zu hinterlassen – die Angriffsmodule bestehen aus Skripten für die Windows PowerShell.

Wer eine Windows-Domäne administriert, sollte Tools wie **mimikatz** kennen, das Anmeldeinformationen aus dem Arbeitsspeicher der Windows-Clients ausliest. Angreifer gelangen damit schlimmstenfalls an die Zugangsdaten eines Domänen-Administrators und können das gesamte Netzwerk übernehmen. Den Domänencontroller spüren die Eindringlinge vorher mit **AdFind** von joeware auf. Auch **PsExec** aus Microsofts SysInternals-Kollektion birgt ein gewisses Missbrauchspotenzial: Es wird genutzt, um Befehle auf anderen Rechnern im Netzwerk auszuführen. Angreifer nutzen es mit

zuvor erbeutete Anmeldeinformationen.

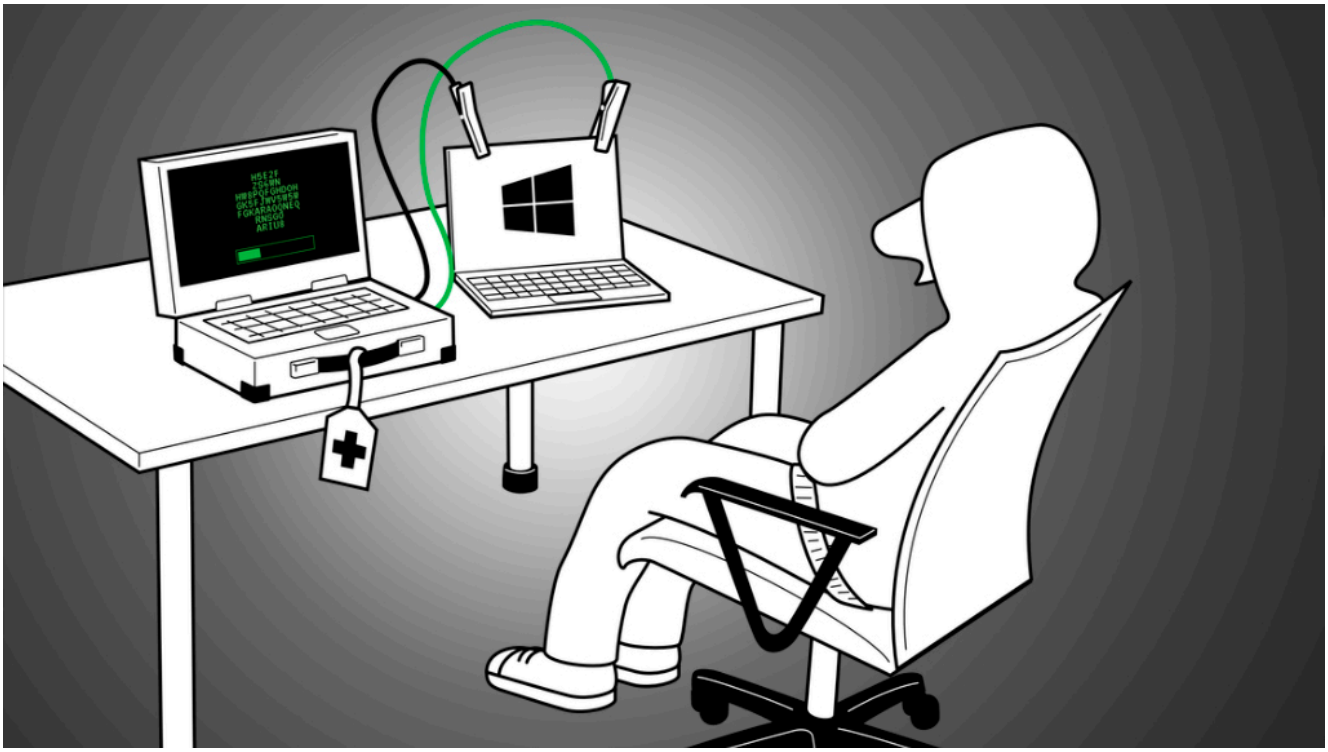
Das von der NSA entwickelte Reverse-Engineering-Toolkit **Ghidra** ist interessant, wenn Sie ausführbaren Code (wie EXE- und DLL-Dateien) bis ins letzte Bit auseinandernehmen und verstehen möchten. Es dekompiliert Binärdateien und kann sie auch wieder zusammenbauen, ähnlich wie der kommerzielle Disassembler IDA Pro. In c't 14/2020 haben wir Ghidra ausführlicher getestet (siehe ct.de/ygg5).

Fazit

Die vorgestellten Hacking-Tools decken einen weiten Bereich ab. Manche Techniken sind erschreckend simpel, andere fordern viel Einarbeitung und Erfahrung. Sich damit zu beschäftigen lohnt sich aber: Sie lernen so, wie ein Angreifer zu denken und Ihre eigenen Sicherheitsprobleme und -lücken aufzuspüren. Das ist hilfreich – ganz gleich, ob Sie nur eine private WordPress-Site betreiben oder gar für die Sicherheit Ihrer Kunden verantwortlich sind. *(rei@ct.de)*

Hacking-Tools & weitere Infos: ct.de/ygg5

Hack Dich selbst – Nützliche Hacking-Tools für den Alltag



Hack Dich selbst

Haben Sie schon mal ein Passwort vergessen oder wichtige Dateien versehentlich gelöscht? Statt darüber zu fluchen, können Sie sich oftmals einfach selbst helfen: Schlüpfen Sie in die Rolle eines Hackers und verschaffen Sie sich wieder Zugriff auf Ihre Daten – ganz legal.
Haben Sie schon mal ein Passwort vergessen oder wichtige Dateien versehentlich gelöscht? Statt darüber zu fluchen, können Sie sich oftmals einfach selbst helfen: Schlüpfen Sie in die Rolle eines Hackers und verschaffen Sie sich wieder Zugriff auf Ihre Daten – ganz legal.

Von Ronald Eikenberg und Alexander Königstein

Hacken Sie Ihren eigenen Rechner: Was erstmal absurd klingt, kann Ihnen das Leben mit der Technik erheblich erleichtern. Denn mit den Werkzeugen der Hacker erledigen Sie nicht nur vieles schneller, Sie können damit auch echte Alltagsprobleme lösen und sich aus der Patsche helfen. Nicht alle Hacking-Tools sind automatisch böse, oftmals handelt es sich um harmlose, aber äußerst nützliche Programme, die spezielle Aufgaben besonders gut oder effektiv lösen.

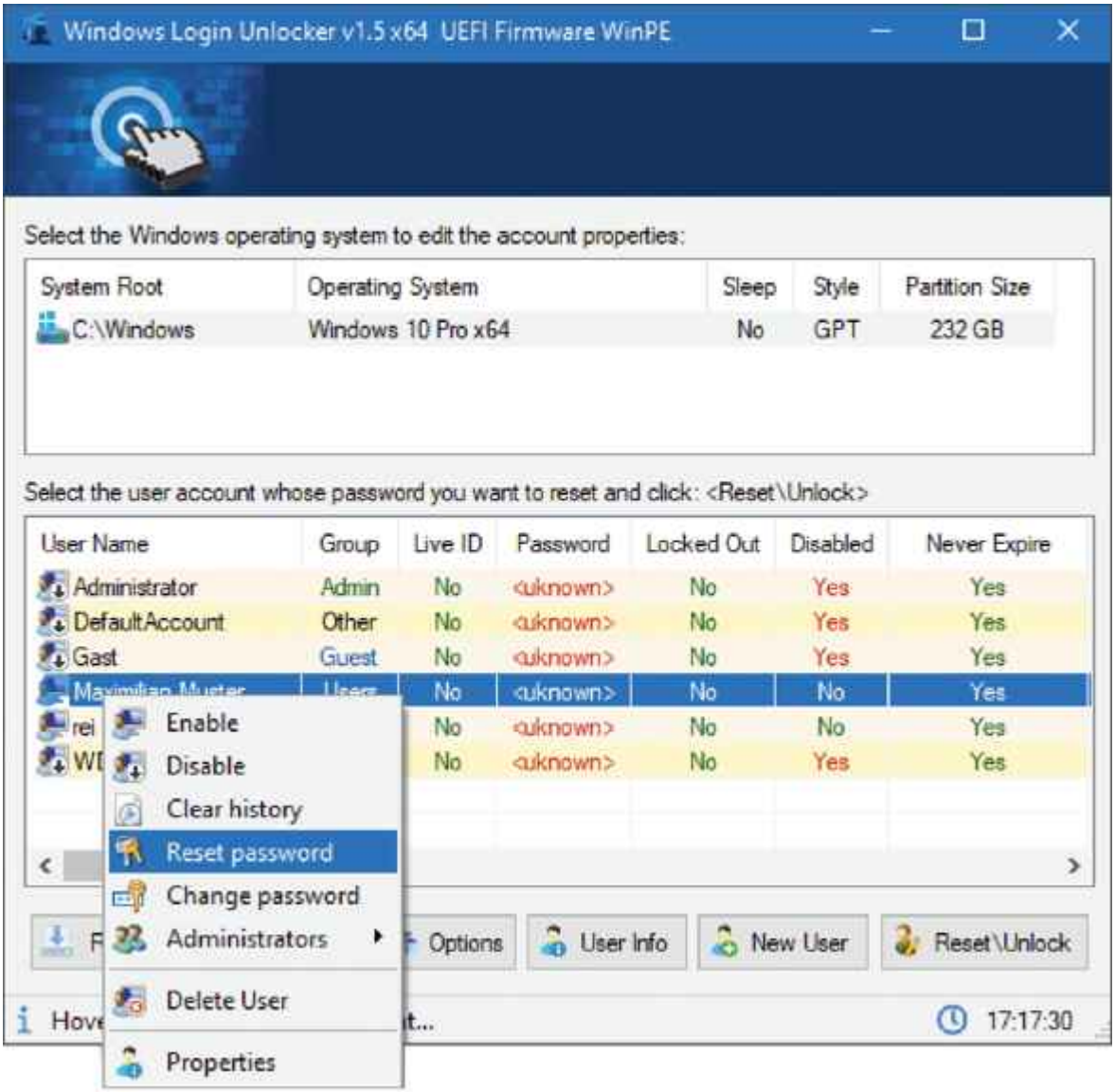
Bei Hackerangriffen ist keine schwarze Magie im Spiel, häufig sind es frei verfügbare Open-Source-Tools, die für sich genommen nicht gefährlich sind. Nach einer Infektion werden sie nachgeladen und automatisiert ausgeführt, um zum Beispiel Dateien oder Passwörter erstmal lokal einzusammeln. Ausgeleitet werden die Daten erst vom eigentlichen Schadcode (oder einem weiteren Tool). Andere Open-Source- Tools laufen direkt bei den Hackern, um zum Beispiel verschlüsselte Daten zu knacken oder gelöschte Dateien zu rekonstruieren.

Die missbräuchlich eingesetzten Werkzeuge werden von vielen Virenwächtern als „HackTool“ erkannt, weshalb den nützlichen Systemhelfern zu Unrecht ein schlechter Ruf anhaftet. Um das zu ändern, stellen wir Ihnen in diesem Artikel einige „Hacking-Tools“ vor, die sich bei uns bewährt haben. Wenn Sie sich erstmal langsam herantasten möchten, können Sie Programme gefahrlos in einer virtuellen Maschine oder auf einem ausgemusterten PC ausprobieren. Die Download-Links zu allen Tools sowie Verweise auf weiterführende c’t-Artikel finden Sie unter ct.de/y41x.

Windows-Passwort zurücksetzen

Anmelden klappt nicht, weil Windows-Passwort vergessen? Kann ja mal passieren. Wenn alle möglichen und unmöglichen Kennwörter durchprobiert sind und auch die Recovery-Fragen nicht weiterhelfen, ist guter Rat teuer. Eine Neuinstallation wäre naheliegend – ist jedoch meist gar nicht nötig. Ist die Systemplatte nicht verschlüsselt, können Sie das alte Passwort, genauer gesagt dessen Hash, einfach überschreiben. Doch Achtung: EFS-verschlüsselte Dateien lassen sich nach dieser Prozedur aus Sicherheitsgründen nicht mehr entschlüsseln (Das Encrypting File System, kurz EFS, ist die transparente Dateiverschlüsselung von NTFS). Der Hash liegt im Registry-Zweig des Security Accounts Managers (SAM), wobei es sich letztlich nur um eine Datei auf der Platte (c:\windows\system32\config\sam) handelt. Die ist allerdings

im laufenden Betrieb stets von Windows geöffnet, sodass Sie sie nicht einfach so bearbeiten können.



Windows-Passwort vergessen? Mit dem Windows Login Unlocker setzen Sie es einfach zurück.

Mit dem **Windows Login Unlocker** aus dem c’t-Notfall-Windows können Sie das Windows-Passwort dennoch zurücksetzen. Sie booten den Rechner vom Stick und der Unlocker übernimmt alle nötigen Schritte für Sie. Mit dem Tool können Sie das Passwort nicht nur zurücksetzen oder gleich ganz entfernen, sie können damit auch Konten anlegen und löschen. Der Unlocker entsperrt sogar Accounts, die mit einem Microsoft-Konto verknüpft sind. Solche werden dabei in ein lokales Benutzerkonto umgewandelt. Einen bootfähigen USB-Stick mit dem Notfall-Windows und dem Unlock-Tool können Sie mit unserer Anleitung in c’t 26/2020

leicht selbst erstellen, alle nötigen Dateien gibt es kostenlos zum Download (siehe ct.de/y41x). Sie finden das Tool im Notfall-Windows unter „Start/Datenrettung“.

Die Bedienung des Unlockers erklärt sich fast von selbst: Oben listet er die gefundenen Windows-Installationen auf, zum Beispiel c:\Windows. Wählen Sie die passende und darunter das Windows-Konto, das Sie retten möchten. Nach einem Rechtsklick haben Sie diverse Möglichkeiten, von denen Sie entweder „Reset“ oder „Change password“ wählen. Die Änderung ist beim nächsten regulären Hochfahren ohne Stick aktiv und Sie können sich wieder einloggen. Alternativ können Sie das etablierte Open-Source-Tool „chntpw“ nutzen, das auch unter Linux läuft. Es ist in Kali Linux (siehe Seite 30) bereits enthalten. Ist das Windows-Konto mit einem Microsoft-Account verknüpft, können Sie es mit chntpw jedoch nicht entsperren.

Nach der Rettungsaktion ist das Windows wieder wie gewohnt nutzbar, allerdings mit einer Ausnahme: Daten, die über die Windows-Funktion CryptProtectData() verschlüsselt gespeichert wurden, können Sie weiterhin nicht entschlüsseln, da dazu das ursprüngliche Passwort nötig ist. Hiervon sind zum Beispiel die Passwortspeicher einiger Browser und durch Windows verschlüsselte Dateien (EFS, siehe oben) betroffen, nicht aber Bitlocker.

Das Unlock-Tool demonstriert anschaulich, dass ein Windows-Konto kein wirksamer Zugriffsschutz ist. Wenn Sie unbefugte Zugriffe verhindern möchten, sollten Sie Ihre Laufwerke zum Beispiel mit BitLocker oder VeraCrypt verschlüsseln. Dann sind nur nicht Ihre Dateien geschützt, sondern auch die Windows-Installation samt Passwort-Hashes (SAM). Das Entschlüsselungskennwort sollten Sie jedoch besser nicht vergessen.

Zugangsdaten einsammeln

Im Laufe eines Windows-Lebens sammeln sich etliche

Zugangsdaten im System an, zum Beispiel im Browser, Mail-Client, VPN-Programm, aber auch alle WLAN-Kennwörter. Auf diese Datenbeute haben es üble Zeitgenossen natürlich abgesehen. Sie nutzen spezielle Programme, um die gespeicherten Logins in Sekundenschnelle einzusammeln. Solche Tools sind für sich genommen völlig harmlos, denn sie übertragen die gefundenen Zugangsdaten nicht, sondern zeigen sie lediglich an und können sie in eine Datei exportieren. Das kann im Alltag sehr nützlich sein, etwa um Zugangsdaten aus einer alten Windows-Installation zu retten, bevor man das System neu aufsetzt.

Schauen Sie sich zunächst im NirSoft-Fundus um: Hier finden Sie Password-Recovery-Tools für fast jeden Zweck, darunter **WebBrowserPassView**, das die Passwortspeicher der gängigsten Browser ausliest. **Mail PassView** liest Zugangsdaten aus Mail-Clients, **VaultPasswordView** aus der Windows-Anmeldeinformationsverwaltung und so weiter. Einen interessanten Zusatznutzen hat das Tool **WirelessKeyView**: Es zeigt nicht nur die im System gespeicherten WLAN-Zugangsdaten an, es kann daraus auch QR-Codes generieren, mit denen Sie Smartphones und Tablets schnell in Ihr WLAN helfen.

Die NirSoft-Tools sind leicht zu bedienen, da ihr Funktionsumfang überschaubar ist. Möchte Sie sich einen Überblick über die Gesamtsituation verschaffen, können Sie zum Python-Tool **LaZagne** greifen, das in einem Durchgang viele Speicherorte von Betriebssystem und Anwendungen durchforstet. Es wird selbst unter Linux und macOS fündig. Laden Sie das Tool am besten als Python-Skriptsammlung (Zip-Datei) von GitHub herunter – es existiert zwar eine direkt ausführbare Windows-Datei, diese konnten wir auf unseren Systemen jedoch nicht starten.

Falls nicht vorhanden, installieren Sie zuerst den Python-Interpreter. Unter Windows aktivieren Sie „Add Python to PATH“ und melden sich nach der Installation neu an, damit die folgenden Befehle funktionieren. Entpacken Sie das Zip-Archiv

von LaZagne und installieren Sie mithilfe der Datei requirements.txt alle nötigen Python-Module: pip install -r requirements.txt. Anschließend wechseln Sie in das Verzeichnis, das zu Ihrem Betriebssystem passt (etwa „Windows“) und können dort LaZagne mit dem folgenden Befehl ausführen: python laZagne.py all Durch das „all“ führt LaZagne sämtliche vorhandenen Analysemodule aus. Wenn Sie es weglassen, erhalten Sie eine Übersicht über die möglichen Befehle.

Hat alles geklappt, liefert Ihnen das Tool eine lange Liste mit Zugangsdaten, Hashes et cetera – abhängig davon, was es auf Ihrem System zu holen gibt. LaZagne kann vieles mit den Rechten eines Standardnutzers auslesen, für manche Dinge – etwa WLAN-Passwörter – benötigt es jedoch Adminzugriff. Falls Sie das ausprobieren möchten, können Sie unter Windows die Eingabeaufforderung per Rechtsklick als Admin öffnen und anschließend LaZagne wie oben beschrieben starten.

Passwörter knacken

Passwortgeschützte Zip-Dateien sind ein einfaches und bewährtes Mittel, um Dateien zu verschlüsseln und so vor neugierigen Blicken zu schützen. Man kann sie fast überall mit Bordmitteln öffnen – sofern man sich noch an das richtige Passwort erinnert. Als Retter in der Not kann der legendäre Passwortknacker **John the Ripper** einspringen. Er versucht, das Passwort durch Durchprobieren zu erraten. Die Erfolgschancen stehen und fallen mit der Länge des Kennworts. Ist es recht kurz, wird John mit etwas Glück schon nach wenigen Sekunden fündig, bei sehr langen Zeichenfolgen können Millionen Jahre ins Land ziehen. Wenn Sie sich an Teile des Passworts oder zumindest an dessen Zusammensetzung erinnern, können Sie die Knackdauer jedoch deutlich reduzieren.

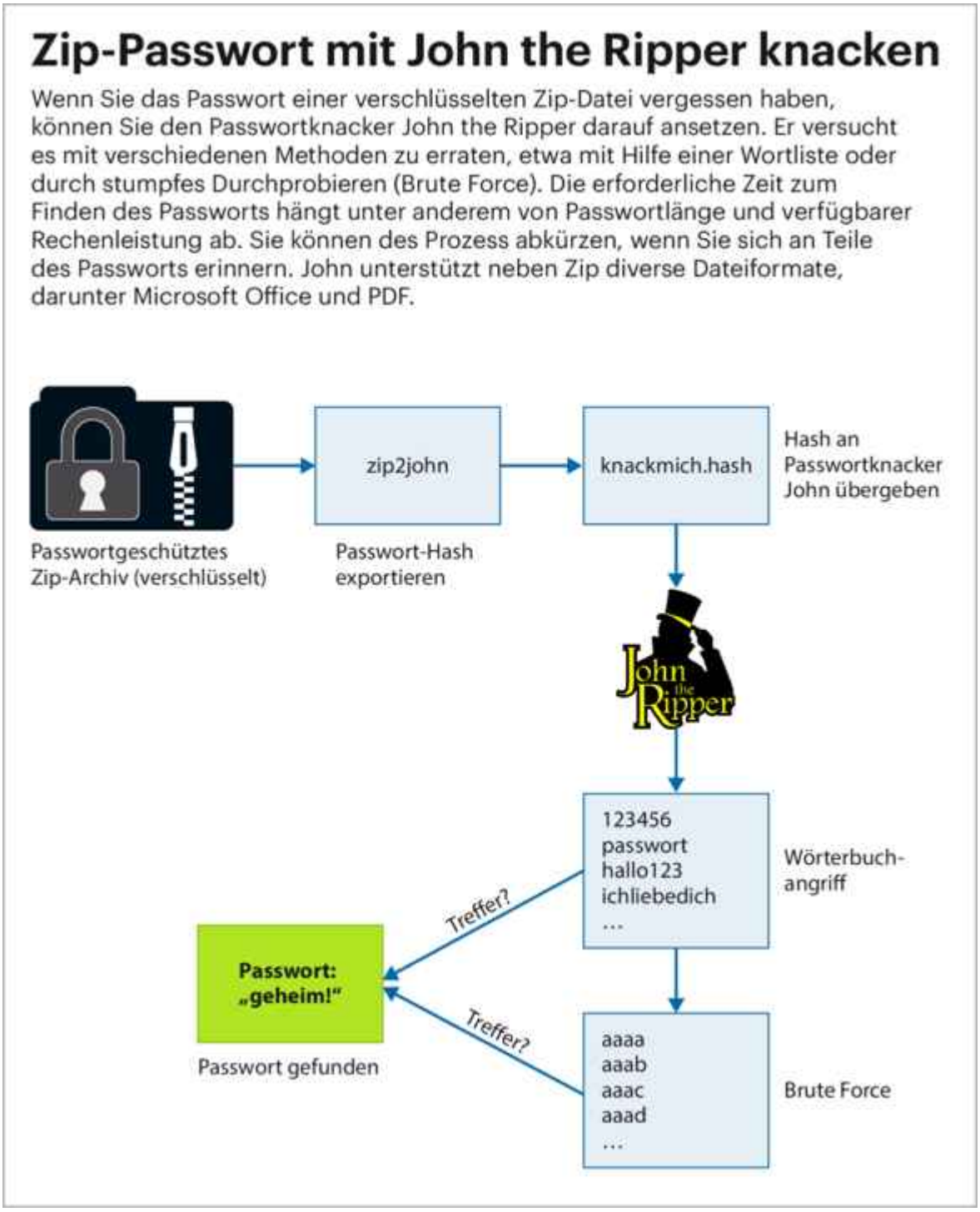
John gibt es für Windows, Linux und macOS, bei Kali Linux (siehe S. 30) ist er bereits an Bord. Er liest die verschlüsselten Dateien nicht selbst ein, er benötigt

stattdessen eine Datei, die den zu knackenden Passwort-Hash enthält. Die können Sie mit den mitgelieferten Hilfswerkzeugen leicht selbst erstellen. Im Lieferumfang befinden sich etliche davon für diverse Dateiformate, darunter neben Zip etwa Android Backup, Bitwarden, KeePass, Office und PDF. Manche Helfer sind Python-Skripte und setzen den dazugehörigen Interpreter voraus. Die Tools liegen im Ordner „run“, Kali-Nutzer schauen indes unter /usr/share/john/.

So weit die Theorie, jetzt folgt die Praxis: Um zum Beispiel ein verschlüsseltes Zip-Archiv mit John zu knacken, extrahieren Sie zunächst den Passwort-Hash mit dem Hilfstool zip2john daraus: zip2john verschluesselt.zip > knackmich.hash. Mit anderen Formaten klappt das ebenso leicht, bei Office-Dokumenten ersetzen Sie zip2john durch office2john, bei PDF-Dokumenten durch pdf2john und so weiter.

Anschließend setzen Sie John auf die Hash-Datei an, im einfachsten Fall mit john knackmich.hash. Dann probiert er zunächst die Kennwörter aus der mitgelieferten Liste password.lst durch, die einige zehntausend der am häufigsten genutzten Passwörter aus dem englischsprachigen Raum enthält. Dabei probiert John gängige Abwandlungen aus, ein Listeneintrag „mutti“ würde deshalb auch das Passwort „Mutti!“ zutage fördern. Das Abarbeiten der Liste dauert nur wenige Sekunden. Mit etwas Glück meldet John nach kurzer Zeit einen Treffer und zeigt das gefundene Passwort auf der Konsole an.

Wird der Passwortknacker noch nicht fündig, probiert er systematisch ASCII-Zeichenkombinationen aus, was deutlich mehr Zeit frisst – und bei langen Passwörtern aussichtlos ist. In diesem Fall sollten Sie den Suchradius möglichst weit eingrenzen.



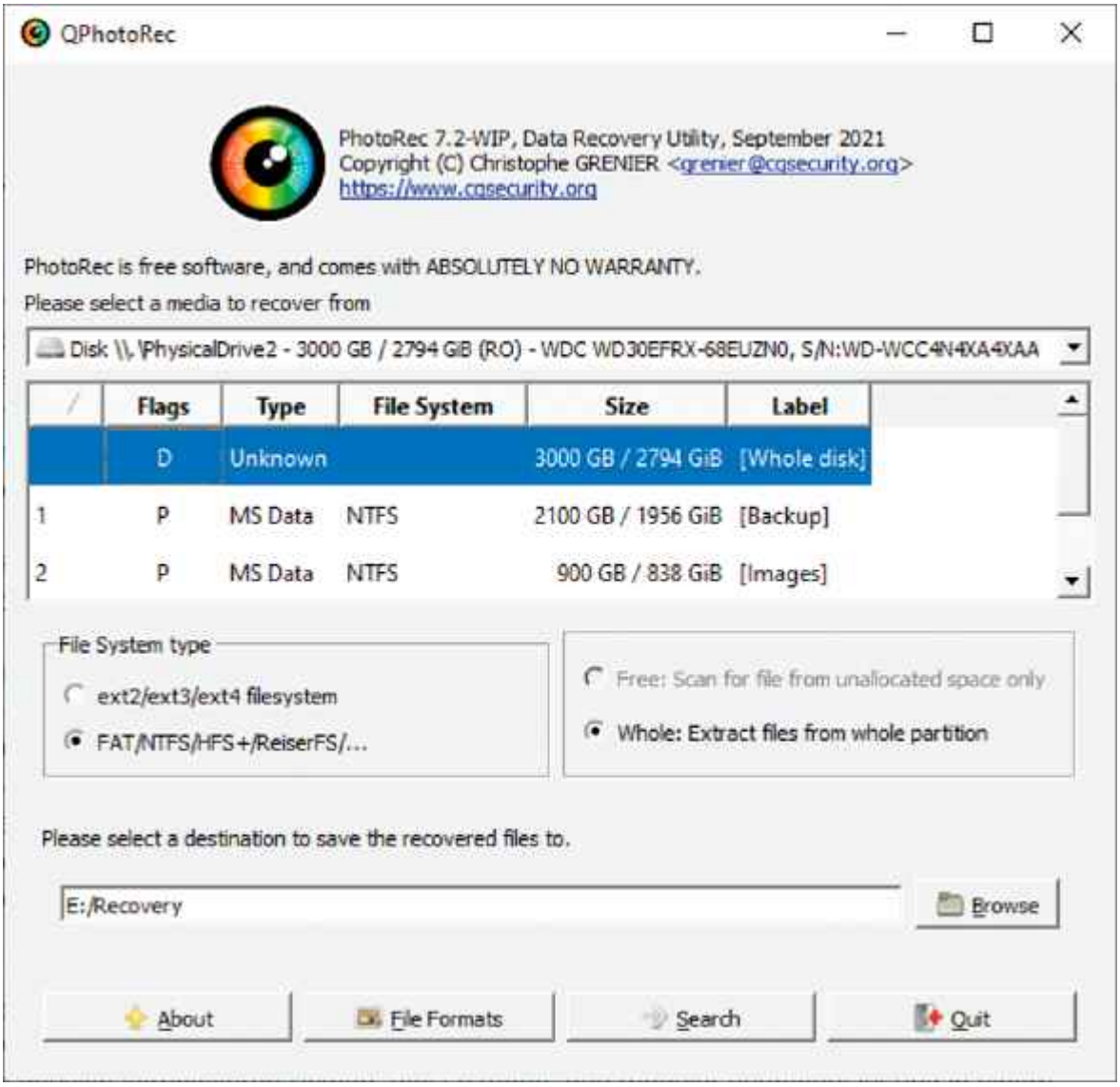
Sie können zum Beispiel eine Mindest- und Maximallänge wie 5 und 6 Zeichen vorgeben, indem Sie -min-length=5 -max-length=6 an den Befehl hängen. Mit -incremental=digits würden Sie den Suchradius auf Ziffern beschränken, um zum Beispiel ein Passwort zu finden, das aus einem Geburtsdatum besteht. Wer einen Teil seines Passworts kennt, sollte John nach einer Passwortmaske suchen lassen. Den Aufbau solcher Masken erklärt die Dokumentation en détail (siehe ct.de/y41x). Im folgenden Beispiel ist bekannt, dass das Kennwort mit „passwort“ beginnt

und darauf noch drei unbekannte Zeichen folgen: john knackmich.hash -mask=passwort?a?a?a

Probieren Sie doch mal aus, wie lange Ihre Kennwörter einem Angriff standhalten würden. Bedenken Sie aber, dass einem echten Angreifer wahrscheinlich mehr Rechenleistung zur Verfügung steht, etwa in Form eines Grafikkarten-Clusters in der Cloud. Zudem setzt er möglichweise eine andere Passwortliste ein, auf der auch Ihr Kennwort steht. Daher gilt: Wählen Sie stets möglichst lange, individuelle Kennwörter – am besten zufällig generiert oder zumindest mit absichtlichen Tippfehlern.

Dateien retten

Gelöschte Dateien sind nicht zwangsläufig unrettbar verloren. Das machen sich Hacker zunutze, um vertrauliche oder pikante Daten von achtlos entsorgten Festplatten, USB-Sticks und Speicherkarten zu kratzen. Die genutzten Tools sind natürlich auch für die Rettung eigener Daten äußerst nützlich – zum Beispiel, wenn Sie wichtige Dateien versehentlich gelöscht haben oder die Daten aus anderen Gründen plötzlich nicht mehr auffindbar sind. Auch Dateien auf SSDs lassen sich mit etwas Glück wiederherstellen, wenn das System den TRIM-Befehl noch nicht ausgeführt hat, um die Daten endgültig zu löschen.



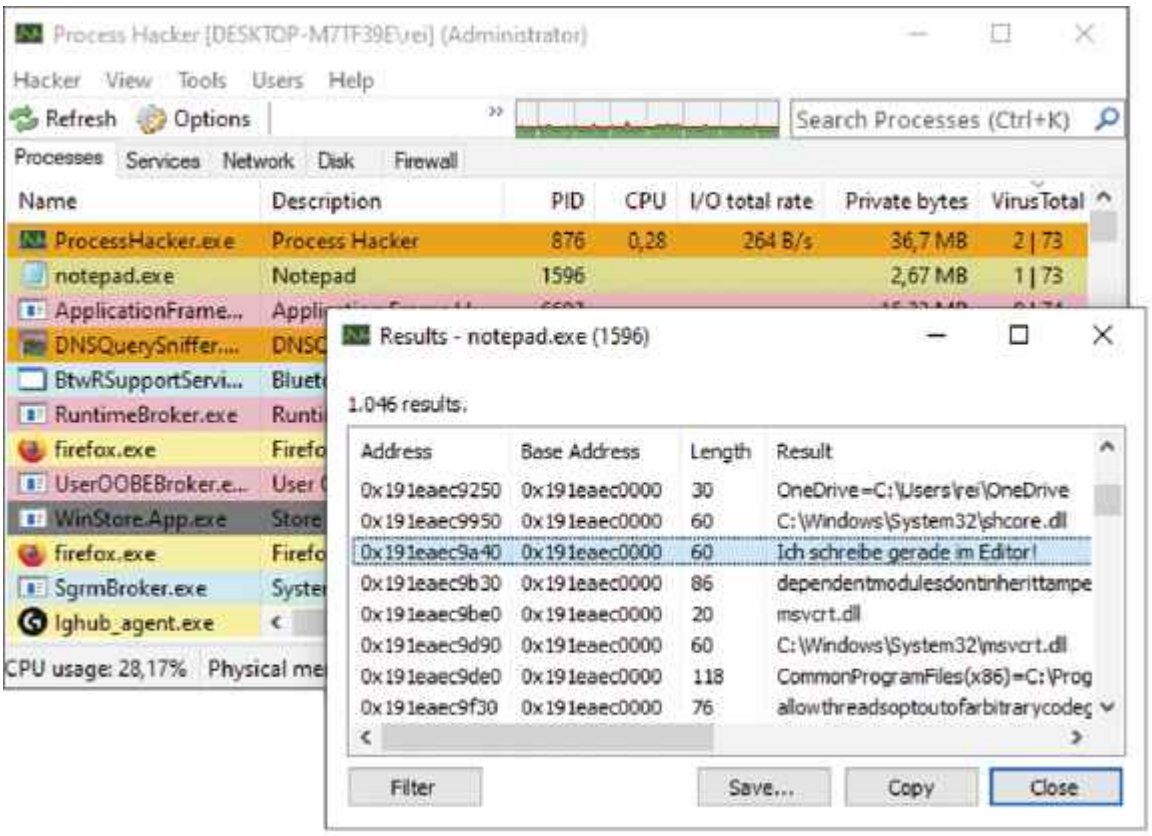
Sind Ihre Dateien noch zu retten? Mit PhotoRec finden Sie es heraus.

Ein bewährtes Werkzeug für diesen Zweck ist das Open-Source-Tool **PhotoRec**, das auf allen möglichen Betriebssystemen läuft. Es ist eigentlich auf der Kommandozeile zu Hause, mit QPhotoRec gibt es inzwischen jedoch auch eine einfache Bedienoberfläche. Nach dem Start wählen Sie oben das zu durchsuchende Laufwerk oder ein Laufwerksabbild und darunter entweder eine bestimmte Partition oder das gesamte Speichergerät. Weiter unten stellen Sie das Dateisystemformat ein und rechts daneben wählen Sie aus, ob nur die unbelegten Speicherblöcke abgesucht werden sollen („Free“) oder alles („Whole“). Zu guter Letzt geben Sie einen Zielordner für die aufgespürten Dateien an und starten die Rettungsaktion mit „Search“.

Falls Ihre Dateien nicht lesbar sind, weil Partitionen oder Dateisystem beschädigt sind, können Sie gezielte Reparaturen daran durchführen. Hierfür greifen Sie am besten zu **TestDisk**, das Sie ohnehin bereits besitzen, wenn Sie PhotoRec heruntergeladen haben. Starten Sie TestDisk über die Konsole, führt es Sie interaktiv durch die wichtigsten Fragen, ehe die Reparatur beginnt. Über die „Undelete“-Funktion können Sie mit dem Tool außerdem gezielt einzelne Dateien wiederherstellen, was schneller zum Ziel führen kann als ein groß angelegter Rettungsversuch mit PhotoRec.

Prozesse hacken

Ein Windows-System gönnt sich selten eine Pause: Prozessor, Datenträger und Netzwerk stehen niemals still. Nur ein Blick hinter die Kulissen zeigt, womit der Rechner gerade beschäftigt ist. Installiert Windows gerade fleißig Updates oder wütet ein Krypto-Trojaner, der alles verschlüsselt, was er in die Finger bekommt? Mit den richtigen Systemtools finden Sie es heraus. Die Auswahl ist riesig, und am bekanntesten sind die SysInternals-Tools, die wir schon ausführlich in c’t präsentiert haben (siehe ct.de/y41x). Im Rahmen dieser Vorstellung von Hacking-Tools möchten wir den Blick auf das Mehrzweck-Tool **Process Hacker** lenken, das einige besondere Extras enthält. Um von diesen Extras zu profitieren, benötigen Sie einen frischen Nightly-Build (3.x).



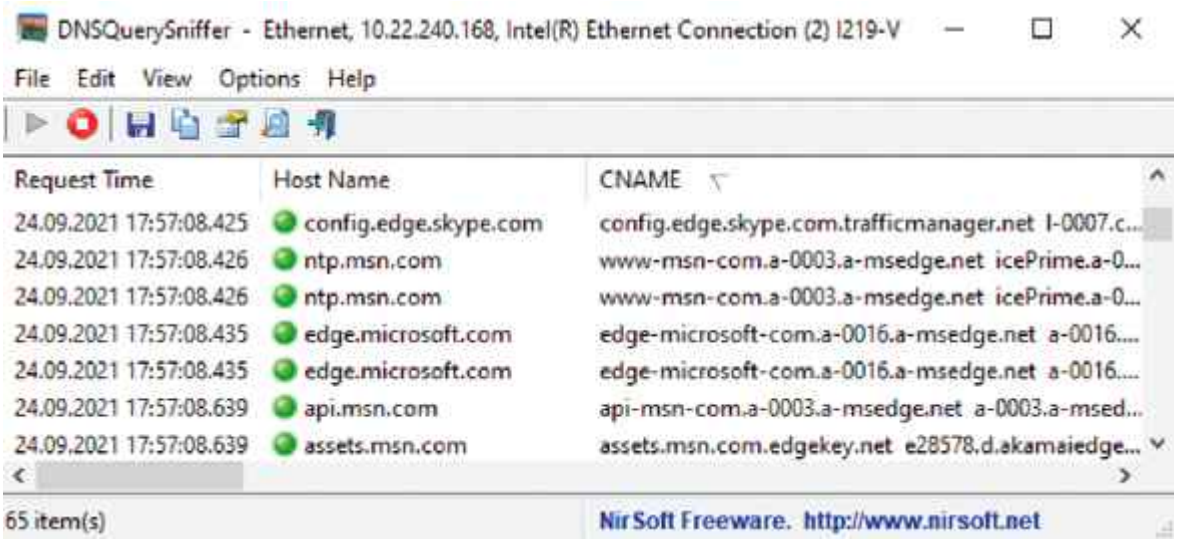
Der Process Hacker macht da weiter, wo andere Taskmanager aufhören: Das Tool erlaubt sogar Eingriffe in den Arbeitsspeicher der Prozesse.
Das Hauptfenster des Process Hacker ist in fünf Tabs unterteilt: „Processes“ zeigt, ähnlich wie der Taskmanager, Informationen über laufende Prozesse an und „Services“ listet die Dienste auf. Über den „Network“-Tab schauen Sie nach, welche Prozesse aktuell mit dem Netz kommunizieren. „Disk“ macht Dateizugriffe sichtbar und „Firewall“ lässt Sie auf die Aktivitäten der Windows-Firewall blicken. Dort sehen Sie, welche aktuellen Verbindungen auf Grundlage welcher Regeln zugelassen oder blockiert wurden. Damit sind nur die Basics beschrieben, es gibt aber noch viel zu entdecken.

Klicken Sie doppelt auf einen Prozessnamen, um ihn unter die Lupe zu nehmen. Hier können Sie zum Beispiel die geladenen Bibliotheken (Modules) einsehen, aber auch im Arbeitsspeicher des Prozesses stöbern (Memory). Klicken Sie dort auf „Options“ und „String“, listet Ihnen Process Hacker sämtliche Zeichenfolgen auf. So können Sie den Speicher zum Beispiel nach Zugangsdaten, IP-Adressen oder API-Schlüsseln

durchsuchen, die das Programm dort bereithält. Über den Tab „Windows“ der Prozesseigenschaften finden Sie heraus, welche Fenster einem Prozess zugeordnet sind und können sogar die einzelnen Fensterelemente verändern. So schalten Sie zum Beispiel – auf eigene Gefahr – gesperrte Buttons frei. Abschließend noch eine kleine Übungsaufgabe: Tippen Sie doch mal einen kurzen Text in den Editor von Windows und ändern Sie das Getippte anschließend, indem Sie den Arbeitsspeicher von notepad.exe mit dem Process Hacker manipulieren.

Netzwerkverkehr untersuchen

Wenn sich Ihr System auffällig verhält, kann sich ein Blick in den Netzwerkverkehr lohnen. Dafür ist **NetworkTrafficView** von NirSoft sehr praktisch: Es zeigt die Netzwerkverbindungen Ihres Systems an und verrät Ihnen, von welchen Prozessen die Verbindungen ausgehen. Aufschlussreich sind auch die DNS-Anfragen, denn bevor eine Verbindung zu einer bestimmten Domain aufgebaut werden kann, muss ein Prozess erstmal die dazugehörige IP-Adresse bei einem DNS-Server erfragen. Mit dem **DNSQuerySniffer**, ebenfalls von NirSoft, können Sie die Anfragen gezielt und live mitverfolgen. So können Sie auch prüfen, ob die DNS-Anfragen Ihres Systems noch im Klartext oder bereits verschlüsselt, etwa über DNS-over-HTTPS (DoH), übertragen werden. In letzterem Fall tauchen sie in dem Analyse-Tool nicht auf.



DNS-Anfragen verraten viel über das Kommunikationsverhalten des Systems. DNSQueryView macht sie sichtbar.
Mit **PacketCache** von Netresec schauen Sie bei der Analyse des Netzwerkverkehrs in die Vergangenheit: Der Dienst schreibt den IPv4-Traffic des Systems fortlaufend in den Arbeitsspeicher, wodurch Sie jederzeit herausfinden können, was in den letzten Minuten passiert ist. IPv6-Verkehr unterstützt er aktuell jedoch nicht. PacketCache wird von Hand eingerichtet, mit den Anweisungen auf der Herstellerseite (siehe ct.de/y41x) ist das jedoch schnell erledigt. Dort erfahren Sie auch, wie Sie die aufgezeichneten Daten abholen, beispielsweise mit dem Analyseprogramm Wireshark oder dem Auswertungs-Tool **NetworkMiner,** das auch von Netresec kommt. Es erlaubt einen schnellen Einblick in die Kommunikation: Wer spricht mit wem, DNS-Anfragen, TLS-Zertifikate und mehr.

Aus Klartextverkehr (HTTP) extrahiert es darüber hinaus Zugangsdaten, URL-Parameter und Bilddateien. Alles, was hier auftaucht, kann auch ein Angreifer sehen, der Ihren Datenverkehr zum Beispiel an einem Hotspot belauscht. Nutzen Sie das Tool, um Datenlecks zu erkennen und gezielt durch Verschlüsselung (etwa per VPN) zu beheben. Wenn Sie mit NetworkMiner live auf den Datenverkehr schauen möchten, sollten Sie den Capture-Treiber Npcap (WinPcap) installieren und als Netzwerkadapter für die Analyse wählen. Die zur Auswahl stehenden „Socket“-Adapter werten lediglich IPv4-Datenverkehr aus, nicht aber IPv6. Wenn Sie Wireshark installiert haben, besitzen Sie den Treiber wahrscheinlich schon.

PowerShell-Hacks

Die Windows PowerShell ist nicht nur ein fester Bestandteil des Betriebssystems, sie ist auch sehr mächtig – und das macht sie für Hacker interessant. Cyberschurken zweckentfremden die PowerShell längst für die feindliche Übernahme einzelner Rechner und ganzer Netzwerke (PowerShell Empire, siehe Seite 29). Aber sie lässt sich auch für nützliche Windows-Hacks

einspannen, etwa um das Betriebssystem individuell zu konfigurieren und seine Geschwätzigkeit zu reduzieren.

Das PowerShell-Modul **Sophia Script** erlaubt Ihnen umfassende Eingriffe ins System, die normalerweise nur sehr umständlich möglich sind. Sie können damit zum Beispiel die Telemetrie- und Diagnosefunktionen zähmen, die Bing-Suche im Startmenü loswerden und den Windows Defender aufmotzen. Die Einrichtung ist bei GitHub ausführlich dokumentiert (siehe ct.de/y41x). In der Zip-Datei befindet sich das PowerShell-Skript Sophia.ps1, das demonstriert, wie Sie die Sophia-Kommandos aneinanderreihen, zum Beispiel um eine frische Windows-Installation nach Ihren Wünschen einzurichten. Führen Sie das Skript erst aus, nachdem Sie es inspiziert und die vorgegebenen Befehle an Ihre Bedürfnisse angepasst haben.

Sie können auch einzelne Funktionen direkt aufrufen. Der folgende Befehl etwa entfernt die Bing-Suche aus dem Startmenü:

```
 . .\Functions.ps1
Sophia -Functions "BingSearch -Disable"
```

Grundsätzlich sollten Sie sich darüber im Klaren sein, was Sie tun und sich über Nebenwirkungen informieren. Wenn Sie etwa Telemetriedienste blockieren, müssen Sie beobachten, ob Windows weiterhin mit Updates versorgt wird. Es gilt die Devise: Weniger ist mehr! Falls Sie unsicher sind, was Sie mit einem Sophia-Befehl auslösen, können Sie einen Blick in den Powershell-Code werfen (Ordner „Module“).

Fazit

Das passende Hacking-Tool zur rechten Zeit kann echte Probleme lösen. Ganz gleich, ob es darum geht, ein vergessenes Passwort zu knacken, verloren geglaubte Dateien zu retten oder nervige Windows-Funktionen abzuschalten. Einigen der Helfer haftet zu Unrecht ein schlechter Ruf an – der Umstand, dass einige davon auch von Cyberschurken genutzt werden, zeigt eher, dass man

mit den Tools sehr effektiv bestimmte Dinge erledigen kann. (*rei@ct.de*)

Tools, Literaturhinweise: ct.de/y41x

Hacking-Tools

Hacking-Tools

Gefährlich, nützlich – oder beides? c’t hat Hacking-Tools ausprobiert, um diese Frage zu klären. Viele entpuppten sich als Problemlöser und können auch Ihnen gute Dienste leisten, etwa um vergessene Passwörter zu knacken, Dateien zu retten oder das Netzwerk auf Sicherheitslücken abzuklopfen.

Die Werkzeuge der Hacker als Problemlöser

Gefährlich, nützlich – oder beides? c’t hat Hacking-Tools ausprobiert, um diese Frage zu klären. Viele entpuppten sich als Problemlöser und können auch Ihnen gute Dienste leisten, etwa um vergessene Passwörter zu knacken, Dateien zu retten oder das Netzwerk auf Sicherheitslücken abzuklopfen.

Von Ronald Eikenberg

Wer Hacker sagt, meint häufig Kriminelle, die unberechtigt Daten kopieren und veröffentlichen. Diese Black-Hats, benannt nach den bösen Cowboys mit schwarzen Hüten aus alten Wildwestfilmen, handeln mit gestohlenen Daten oder betrügen auf Kosten ihrer Mitmenschen. Doch es gibt auch Hacker, die ihr Know-how legal und moralisch einwandfrei einsetzen. Diese White-Hats sind gefragte Leute, sie spüren zum Beispiel als gut bezahlte Penetrationstester (Pentester) Sicherheitslücken für Unternehmen auf.

Allen Hackern gemein ist, neben ihrem technischen Know-how, dass sie sich die Arbeit oft mit speziellen Programmen erleichtern, um viele Aufgaben überhaupt erst erledigen zu können. Viele dieser Hacking-Tools sind frei verfügbar und völlig legitim einsetzbar – es besteht daher kein Grund, sie zu verteufeln. Es spricht sogar vieles dafür, die Tools selbst zu benutzen und damit die Sicherheit der eigenen Rechner, Router & Co. zu untersuchen – oder die eines Auftraggebers. Wer damit jedoch gegen geltende Gesetze verstößt und fremde Systeme attackiert, macht sich natürlich strafbar. Eine fundierte Einordnung der rechtlichen Lage finden Sie auf Seite 170.

Retter in der Not

Wir haben zahlreiche Hacking-Tools ausprobiert und stellen in dieser Ausgabe eine Auswahl der interessantesten Programme vor, die sogar das Zeug zum Retter in der Not haben. Viele der Hacking-Tools starten direkt unter Windows und sind dank einer grafischen Bedienoberfläche verhältnismäßig leicht bedienbar, während andere alle Klischees erfüllen und nur auf der textbasierten Linux-Shell laufen. Wir möchten Ihnen die ganze Bandbreite zeigen: Im folgenden Artikel finden Sie nützliche Helfer für den Windows-Alltag mit konkreten Tipps zur Verwendung. Ist zum Beispiel die Abgabe der Bachelorarbeit gefährdet, weil Sie das Passwort der Word-Datei vergessen haben, setzen Sie doch mal den Passwortknacker **John the Ripper** darauf an. Mehr dazu lesen Sie auf Seite 20. Haben Sie sich aus Ihrem Windows ausgesperrt, setzen Sie das Passwort mit dem **Windows Login Unlocker** einfach zurück. Auf Seite 18 erfahren Sie wie.

Sie helfen Ihren Schwiegereltern beim Umstieg auf einen neuen PC, aber das vor Jahren eingerichtete WLAN-Passwort ist nicht mehr auffindbar? Mit Tools wie **LaZagne** (S. 19) lesen Sie es vom alten Rechner aus und exportieren dabei gleich noch viele andere Zugangsdaten, die sich dort im Laufe der Zeit angesammelt haben und den Umzug beschleunigen. Auf Seite 22 zeigen wir außerdem, wie Sie vermeintlich unrettbar verlorene Dateien wieder ans Tageslicht befördern.

Security-Check

Ab Seite 24 geht es etwas härter zur Sache mit Spezialtools, mit denen zwar nicht jeder etwas anfangen kann, die jedoch erstaunliche Fähigkeiten haben. Mit dem vielseitigen Netzwerkscanner **Nmap** (S. 25) verschaffen Sie sich schnell einen Überblick über die Situation in Ihrem Netzwerk und entdecken vielleicht auch den Nachbarn, der seit der letzten Party immer noch im WLAN mitsurft. Im gleichen Durchgang

können Sie Ihre Geräte auf Sicherheitsprobleme abklopfen.

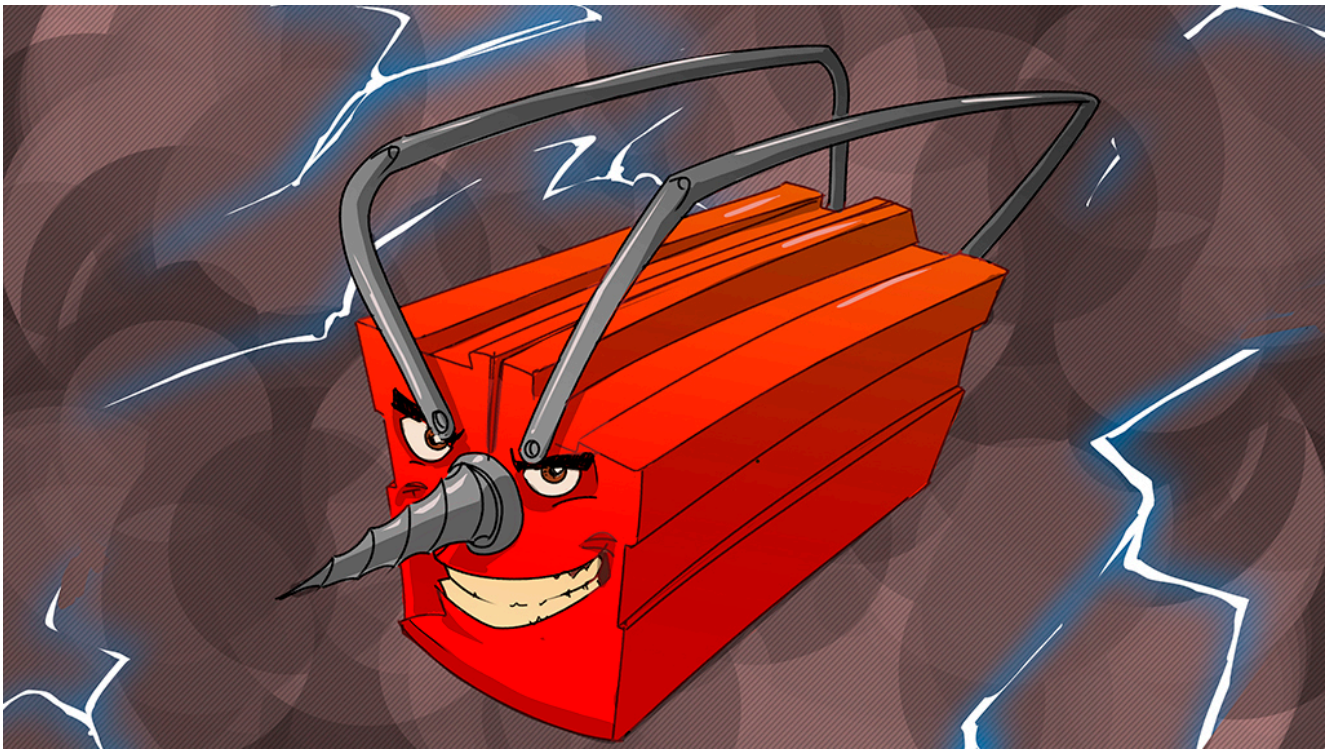
Machen Sie Bekanntschaft mit Hydra, Medusa und John the Ripper: Hacking-Tools mit gefährlich klingenden Namen sind, richtig eingesetzt, echte Problemlöser.

WordPress-Websites stehen unter Dauerfeuer, weil Angreifer nur zu gut wissen, dass ein verpenntes Sicherheits-Update ausreicht, um den ganzen Server zu übernehmen. Auch veraltete und verwundbare Erweiterungen sind schon vielen WordPress-Betreibern zum Verhängnis geworden. Wenn Sie das gleiche Werkzeug wie die Angreifer nutzen, spüren Sie etwaige Sicherheitslücken rechtzeitig auf und können Gegenmaßnahmen ergreifen, bevor Ihre Daten im Darknet gehandelt werden. Blättern Sie hierfür zu **WPScan** auf Seite 27.

Last, but not least, zeigen wir Ihnen ab Seite 30, wie Sie sich einen bootfähigen Hacking-Stick erstellen. Als Grundlage dient **Kali Linux**, das etliche Security-Tools enthält, die Sie direkt ausprobieren können. Alles, was Sie brauchen, ist ein USB-Stick mit mindestens 8 GByte und etwas Zeit. Manche der Tools sind zwar etwas unhandlich, von dem gewonnenen Fachwissen können Sie jedoch lange profitieren. Genau das

Richtige für verregnete Herbsttage. (*rei@ct.de*)

Rechtliche Unsicherheiten bei Hacking-Werkzeug



Kommt drauf an, wozu

Um Schwachstellen im eigenen Netz zu suchen und Datenflüsse zu überwachen, nutzen Administratoren vielfach die gleichen Softwarehilfsmittel wie Angreifer, die illegale Ziele verfolgen. Was sagt das deutsche Recht dazu? Steht jemand, der mit trickreichen Analyse- und Spähtools arbeitet, mit einem Bei…

Kommt drauf an, wozu

Rechtliche Unsicherheiten bei Hacking-Werkzeug

Um Schwachstellen im eigenen Netz zu suchen und Datenflüsse zu überwachen, nutzen Administratoren vielfach die gleichen Softwarehilfsmittel wie Angreifer, die illegale Ziele verfolgen. Was sagt das deutsche Recht dazu? Steht jemand, der mit trickreichen Analyse- und Spähtools arbeitet, mit einem Bein vor Gericht?

Von Verena Ehrl

Der Theaterautor und Sprachliebhaber Hans-Joachim Haecker brachte die Dual-Use-Problematik bereits 1968 in einem Gedichtchen seines Bandes „Insonderheit“ unter dem Eindruck des internationalen Wettrüstens scherzhaft auf den Punkt:

„Insonderheit die Abwehrwaffen
sind für die Abwehr wie geschaffen.
Auch kann man mit geschickten Händen
sie für den Angriff gut verwenden.“

Die Waffen, mit denen Akteure innerhalb der IT-Welt hantieren, eignen sich zum Eindringen in Systeme, zum Überwinden von Sicherungsmaßnahmen, zum Spionieren und Manipulieren. Dieselben Werkzeuge können aber dazu dienen, unterschiedliche Ziele zu erreichen. In der Hand eines Administrators, der ein System, für das er verantwortlich ist, Penetration Tests („Pentests“) aussetzt, kann etwa das Software-Tool „Mimikatz“ legalen Einsatz finden (S. 24). Es ebnet allerdings ebenso gut Angreifern den Weg bei illegalen Aktionen, indem es ihnen Zugangsdaten für die Übernahme eines Netzwerks offenbart. Auf diese Ambivalenz bezieht sich das Schlagwort „Dual Use“ im Zusammenhang mit Hackerausrüstung.

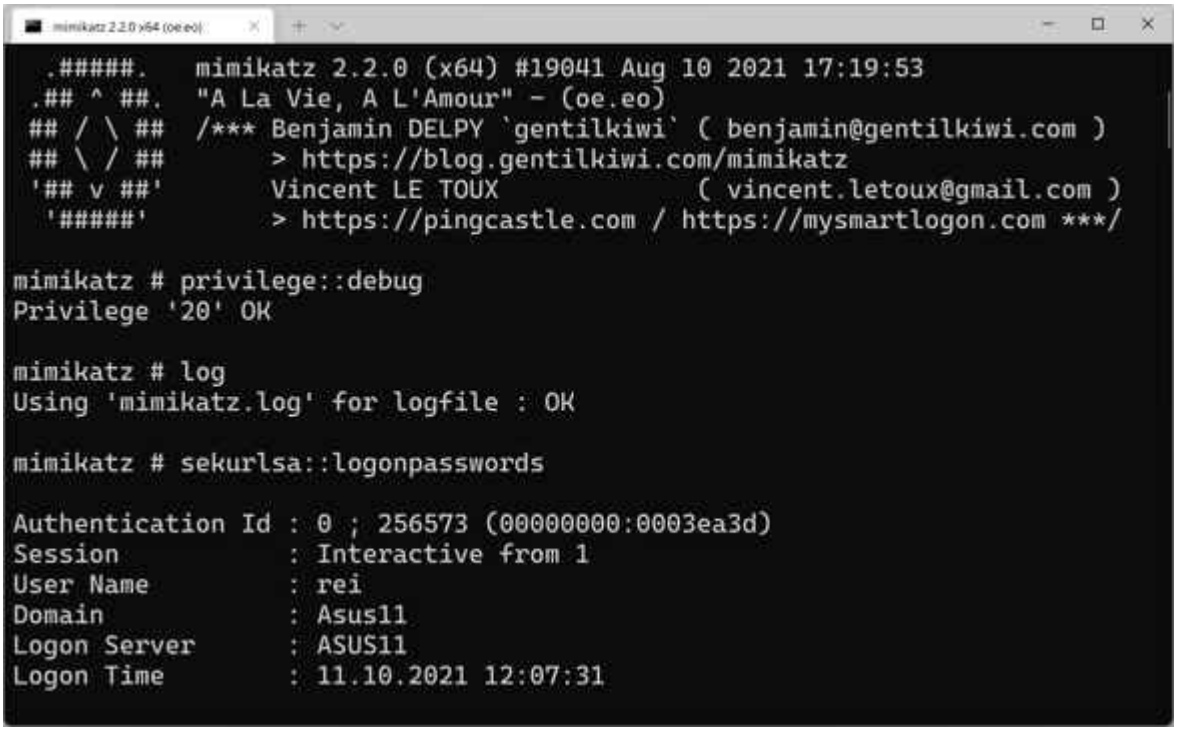
Nicht immer erscheinen die Werkzeuge, um die es geht, so spektakulär wie die Hacking-Gadget-Hardware, mit der c’t sich

in Ausgabe 18/2017 befasst hat [1]. Sehr oft steht vielmehr bloße Software im Mittelpunkt, die loggt, sucht, entschlüsselt, ausliest, analysiert und speichert (S. 16, 18, 24 und 39). Die rechtlichen Fragen, vor die ein Anwender gestellt ist, sind jedoch grundsätzlich die gleichen wie bei den Spionagegerätchen [2]: Wo liegt die rote Linie, jenseits der man sich auf illegalem Terrain bewegt? Was sagt das geltende Recht zum Umgang mit potenziell gefährlichen und schadenträchtigen Tools?

Dass es „Güter mit doppeltem Verwendungszweck“ gibt, die sich gleichermaßen für legales und illegales Tun eignen, beschäftigt nicht zuletzt den europäischen Gesetzgeber. Am 9. September 2021 ist die Neufassung der sogenannten Dual-Use-Verordnung in Kraft getreten [3].

Sie betrifft „Güter einschließlich Datenverarbeitungsprogramme (Software) und Technologie, die sowohl für zivile als auch für militärische Zwecke verwendet werden können“. Es gibt durchaus Softwareentwicklungsprojekte, die man mit etwas Fantasie in den Betrachtungshorizont der Verordnung rücken kann.

Ziel der Dual-Use-Verordnung ist die Exportkontrolle. Die kann bereits relevant werden, wenn Forschung und Produktentwicklung mit Partnerunternehmen in bestimmten außereuropäischen Ländern stattfinden und dabei schadenträchtige Software im Spiel ist.



Mimikatz ist ein typisches Beispiel für ein Hackerwerkzeug, das auch verantwortungsvollen Admins wertvolle Dienste leistet, wenn es ums Aufspüren von Schwachstellen im eigenen Netz geht.

Neu im Blick der europäischen Rechtssetzungsorgane und der zur Umsetzung verpflichteten Mitgliedsstaaten sind Länder, welche die Todesstrafe praktizieren oder in denen Menschenrechtsverletzungen wie Folter auf staatliches Geheiß stattfinden. Wer etwa potenziell gefährliche Software ins nichteuropäische Ausland transferieren will, braucht dazu eine vorherige Genehmigung des Bundesamts für Wirtschaft und Ausfuhrkontrolle (BAFA). Diese Behörde entscheidet in jedem Einzelfall, ob der Transfer zulässig ist oder nicht.

Zweierlei Paar Schuhe

Abseits der von der Verordnung erfassten Transferproblematik sind Dual-Use-Softwarewerkzeuge rechtlich schwer zu fassen. Weder ihr Erwerb noch ihr Besitz ist grundsätzlich untersagt. Straf- und Zivilrecht melden sich erst dann, wenn jemand diese Tools einsetzt, um Rechtsbrüche zu begehen. Derjenige riskiert dann eine Strafe oder er sieht sich zivilrechtlichen Ansprüchen ausgesetzt – oft droht ihm beides.

Nicht alles, was jemand rechtswidrig tut, ist auch strafbar. Mit dem Strafrecht geht der Staat gegen von ihm untersagtes Verhalten vor, dabei sind Strafermittlungsbehörden im Spiel, es gibt Beschuldigung und Anklage. Im Zivilrecht stehen hingegen gleichberechtigte Streitparteien einander gegenüber. Dabei gibt es Kläger und Beklagte, die Gerichte entscheiden über Ansprüche, welche die Parteien gegeneinander geltend machen. Vertragspflichten und Schadenersatzansprüche sind typisches zivilrechtliches Geschäft.

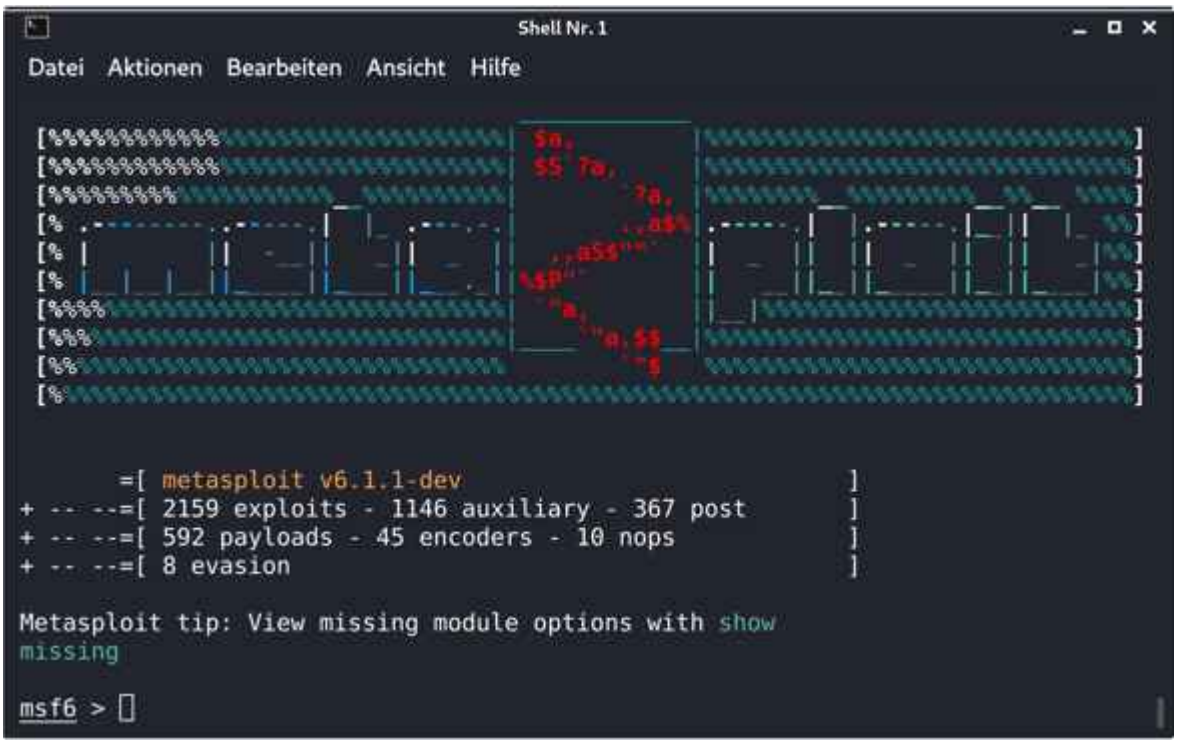
Durch Software kann ein Anwender sich Ärger in beiden Rechtsbereichen einhandeln. Ein gutes Beispiel für die rechtliche Gratwanderung dabei sind die bereits angesprochenen Pentests. Sie haben die Aufgabe, Schwachstellen in Konfiguration, Hard- und Software von Servern, Routern und Arbeitsplätzen im Netz aufzuzeigen. Ein Mitarbeiter, der einen solchen Test im Auftrag eines zuständigen Entscheiders für das betroffene Netz durchführt, bewegt sich damit auf der legalen Seite. Wenn allerdings etwa ein Cybersecurity-Dienstleister einen Pentest unaufgefordert und ohne Erlaubnis bei einem potenziellen Kunden durchführt, um diesen als Auftraggeber zu gewinnen, setzt er sich strafrechtlicher Verfolgung wegen Datenveränderung oder Computersabotage aus.

Wesentlich sind dabei die Paragrafen 303a und 303b des Strafgesetzbuchs (StGB), die sich mit virtueller Sachbeschädigung befassen. Damit hat der Gesetzgeber 1986 eine Regelungslücke beim Straftatbestand der Sachbeschädigung (§ 303 StGB) geschlossen. Die klassische Sachbeschädigung setzt einen körperlichen Gegenstand voraus – das lässt Daten und beispielsweise Festplatten, die funktionsfähig bleiben, aber deren Inhalt gelöscht oder verschlüsselt wurde, außen vor.

§ 303a StGB stellt die unbefugte Veränderung von Daten unter Strafe. Dort heißt es in Absatz 1: „Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.“

Bereits der Versuch ist strafbar; dasselbe gilt wie beim Ausspähen (§ 202a StGB) und Abfangen von Daten (§ 202b StGB) auch fürs „Vorbereiten“ einer rechtswidrigen Datenveränderung – beispielsweise durch Bereitstellen von Software, deren „Zweck die Begehung einer solchen Tat ist“ (§ 202c Abs. 1 Nr. 2 StGB).

Als Daten in diesem Sinne gelten nach § 202 StGB „nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden“, also nicht etwa Papiernotizen.



Das modulare Pentesting-Tool Metasploit ist bei Security-Experten beliebt, es lässt sich aber auch für echte Angriffe missbrauchen.

§ 303b StGB, der sogenannte Hackerparagraf, ist der Computersabotage gewidmet. Er steht in direktem Zusammenhang mit seinem Nachbarn, der die Datenveränderung betrifft, und lautet: „Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, … erheblich stört, … wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“

Wenn es um die Datenverarbeitung eines Unternehmens respektive

einer Behörde geht, stehen Freiheitsstrafen bis zu fünf Jahren im Raum. In besonders schweren Fällen riskieren Täter sogar bis zu zehn Jahren Gefängnis. Der Paragraf grenzt die Wege, auf denen die strafbare Datenverabeitungsstörung bewirkt wird, näher ein: Unter Nr. 1 fasst er die Störung durch Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten (siehe § 303a Abs. 1). Unter Nr. 2 erscheint die Dateneingabe und -übermittlung mit der Absicht, jemand anderem einen Nachteil zuzufügen. Unter Nr. 3 schließlich geht es darum, dass eine Datenverarbeitungsanlage oder ein Datenträger zerstört, beschädigt, unbrauchbar gemacht, beseitigt oder verändert wird. Auch hierbei sind wie bei der Datenveränderung bereits Versuch und Vorbereitung strafbar.

Dass es nur ums Stören von Datenverarbeitungen von „wesentlicher Bedeutung“ geht, soll Bagatellfälle aus dem Blick der Strafjustiz nehmen.

Erpressungstrojaner vor Gericht

Im April 2021 hat der Bundesgerichtshof (BGH) einen Fall entschieden, der die Verteilung von Ransomware betraf – also das Einschleusen von Verschlüsselungstrojanern zu Erpressungszwecken [4]. Dabei stufte das Gericht unter anderem das Anbringen einer Eintragung in der Windows-Registry, die das automatische Laden einer Schadsoftware beim Rechnerstart bewirkte, als strafbare Datenveränderung ein. Zugleich sah der BGH in diesem Fall auch eine Computersabotage nach § 303b StGB.

Der Angeklagte war Mitglied einer Cybercrime-Bande mit Sitz in der Ukraine. Diese hatte mit ihren Ransomware-Angriffen von 2013 bis 2016 über 200 Millionen Rechnersysteme infiziert und von den geschädigten Computernutzern mehr als neun Millionen Euro erpressen können.

Schadsoftware ähnlicher Art mit einer vorgesehenen Entsperrmöglichkeit hätte aber auch im Rahmen eines Pentests

in einem lokalen Netz durchaus legal verwendet werden können. Ein Unternehmen hätte damit etwa seine Mitarbeiter auf deren Vorsicht testen können, was das Anklicken unbekannter Inhalte betrifft.

Computersabotage am Arbeitsplatz

Das mutwillige Stören des Datenverarbeitungsbetriebs kann nicht nur strafrechtliche, sondern auch arbeitsrechtliche Auswirkungen haben. Mitarbeiter, die aus Wut oder infolge von Rachegedanken gegen ihren Arbeitgeber Datenvandalismus im Unternehmensnetz betreiben, riskieren eine fristlose Kündigung.

Das geschah 2019 einem als Key-Account-Manager beschäftigten Arbeitnehmer nach einer heimlichen Löschaktion auf dem Unternehmensserver seines Arbeitgebers. Nach einer Abmahnung war ihm zuvor ein Aufhebungsvertrag angeboten worden. Daraufhin löschte er 8 GByte an Daten, darunter Kalkulationssoftware, Umsatzmeldungen, Vorlagen für Preislisten und Wettbewerbsanalysen für bestimmte Produkte. Die Daten konnten später wiederhergestellt werden. Der Verdacht fiel auf ihn. Gegen die fristlose Kündigung , die er wenig später erhielt, wehrte er sich zunächst erfolgreich. In der Berufungsinstanz jedoch unterlag er vor dem Landesarbeitsgericht (LAG) Baden-Württemberg im September 2020 [5]. Sein Arbeitgeber hatte einen 93seitigen Vergleich des Datenbestands im fraglichen Verzeichnis vor und nach der Löschaktion vorgelegt.

Das Gericht sah die fristlose außerordentliche Kündigung als begründet an: Das unbefugte vorsätzliche Löschen betrieblicher Daten auf EDV-Anlagen des Arbeitgebers tauge ebenso wie das Vernichten von Verwaltungsvorgängen grundsätzlich als „wichtiger Grund“ für eine solche Kündigung im Sinne des § 626 Abs. 1 BGB. Dabei komme es nicht unbedingt darauf an, ob sich der Arbeitnehmer nach § 303a StGB oder § 303b StGB strafbar gemacht habe. Es sei auch nicht entscheidend, ob und mit

welchem Aufwand ein Teil der gelöschten Daten wiederhergestellt werden konnte oder ob der Arbeitgeber diese Daten für den weiteren Geschäftsablauf tatsächlich benötigte. Vielmehr gehöre es zu den vertraglichen Nebenpflichten eines Arbeitsverhältnisses im Sinne des § 241 Abs. 2 BGB, dass der Arbeitnehmer seinem Arbeitgeber den Zugriff auf betriebliche Dateien nicht verwehre oder unmöglich mache.

In der Hand von Angreifern kann auch der Fern Wifi Cracker, mit dem man Drahtlosnetze auf Sicherheitslücken abklopft, zum Werkzeug für eine Straftat werden.

Wenn der Admin spioniert

Dass es bei der strafrechtlichen Bewertung von Hacker-Aktivitäten nicht so sehr um die benutzten Werkzeuge als vielmehr um Zweck und Absicht des Einsatzes geht, illustriert auch ein Fall, den 2020 der BGH in letzter Instanz entschied [5]. Zwei Männer mussten sich wegen des Ausspähens von Daten (§ 202a StGB) verantworten. Einer davon leitete die Stabsstelle eines Apothekerverbandes und betrieb daneben ein gesundheitspolitisches Informationsportal im Internet. Der zweite Angeklagte arbeitete als Systemadministrator am Berliner Standort des Bundesgesundheitsministeriums (BMG) und war nebenbei als Callboy tätig – daher rührte auch die Bekanntschaft der beiden Männer.

Der Admin hatte jahrelang Zugriffsrecht auf alle E-Mail-Accounts seiner Dienststelle und versorgte den Portalbetreiber mit so gewonnenen Interna aus dem Ministerium. Nachdem das Ministerium den unbeschränkten Mailzugriff der Administratoren im Hause als Sicherheitsmangel erkannt hatte, wurde es für den Mann schwieriger – er verlegte sich schließlich auf einen unter den Admins bekannten Notfalltrick, mit dem er sich selbst von Fall zu Fall die nötigen Zugriffsrechte verschaffte. Er lieferte dem Portalbetreiber auf Datenträger kopierte E-Mail-Inhalte nach Wunsch und kassierte dafür insgesamt rund 1000 Euro. Sein Kunde war besonders an E-Mails der Minister und Staatssekretäre sowie einiger Abteilungs- und Referatsleiter interessiert. In den weitergereichten Mails ging es unter anderem um Gesetzesvorhaben, die für das Publikum des Portals besonders interessant waren.

Das Landgericht (LG) Berlin verurteilte die Männer im April 2019 wegen gemeinschaftlichen Ausspähens von Daten nach § 202a StGB und sah in der Manipulation der Zugriffsrechte auf die einzelnen E-Mail-Konten zudem die Überwindung einer Zugangssicherung nach § 202a Abs. 1 StGB. Die gegen das landgerichtliche Urteil eingelegte Revision wies der BGH

weitgehend ab, lediglich den einzuziehenden Geldbetrag setzte er niedriger an als die Vorinstanz.

Die Bundesrichter beschäftigten sich vor allem damit, ob Daten im Sinn des §202a Abs. 1 StGB überhaupt als gesichert gelten können, wenn ein Admin mithilfe seiner Kenntnisse darauf zugreifen kann. Die Antwort: Es genüge, wenn getroffene Vorkehrungen den Zugriff auf Daten zumindest deutlich erschweren. Die Sicherung von E-Mail-Accounts durch Passwörter reiche aus. Dabei brauche der Systembetreiber nur den Zugriff Unbefugter zu berücksichtigen, aber nicht die Zugriffsmöglichkeit durch Eingeweihte oder Experten. Es sei nicht erforderlich, dass die Sicherung gerade gegenüber dem Täter wirkt – wenn dieser etwa ein Administrator ist, der den tatsächlichen Zugriff auf die Daten hat.

Als Überwinden der Zugangssicherung nach § 202a StGB können dem Gericht zufolge auch Handlungen gelten, die nicht besonders anspruchsvoll oder aufwendig sind. Wenn jemand durch Insiderkenntnisse oder Ähnliches eine Absicherung schnell und leicht ausschalten kann, zähle das rechtlich ebenso, als hätte sich jemand durch raffinierte technische Werkzeuge Zugriff verschafft. Nur wenn eine Durchbrechung des Schutzes für jedermann ohne Weiteres möglich sei, werde der Tatbestand nicht erfüllt.

Wer den Schaden hat …

Wie bereits gesagt, ist strafrechtliche Verfolgung nicht das Einzige, was der illegale Einsatz von Hacking-Tools nach sich ziehen kann: Wenn dabei ein Schaden entsteht, hat der Geschädigte einen Anspruch auf Schadenersatz gegen den Verursacher. Schäden durch IT-Störmanöver können sehr hoch sein – wenn etwa durch den Ausfall von Unternehmensservern Arbeitsprozesse lahmgelegt werden. Auch der Ausfall der Netzkommunikation kann enorme Umsatzeinbußen und damit hohe wirtschaftliche Schäden bedeuten. Für Anspruchsteller im Zivilrecht ist wichtig, dass jede Streitpartei alles, was für

ihre Sache spricht, selbst gerichtsfest beweisen muss. Das kann bei Schäden durch Hackertools etwa den Nachweis eines Hackerangriffs und die zweifelsfreie Benennung des Angreifers betreffen. Außerdem ist auch nachzuweisen, dass der Angriff tatsächlich den geltend gemachten Schaden hervorgerufen hat.

Wenn ein Täter bereits strafrechtlich wegen einer Computerstraftat zulasten eines Geschädigten verurteilt worden ist, hat jener es anschließend vergleichsweise leicht, seine Ansprüche gegen den Verurteilten zivilrechtlich geltend zu machen: Das Urteil des Strafgerichts hat selbst bereits Indizwirkung, zudem kann der Kläger die im Strafverfahren erhobenen Beweise zu seinen Gunsten nutzen.

Ein dritter, bislang noch nicht genannter Bereich, der durch unrechtmäßigen Einsatz von Hackertools berührt werden kann, ist der Datenschutz. Wo bei einem Angriff personenbezogene Daten im Spiel sind, geht es nicht bloß um wirtschaftliche Schäden, sondern möglicherweise auch um die massenhafte Verletzung des informationellen Selbstbestimmungsrechts der Betroffenen. Wer es also als Pentester mit realen Datenbeständen zu tun hat, tut gut daran, die Bestimmungen der europäischen Datenschutzgrundverordnung (DSGVO) sorgfältig zu beachten. *(psz@ct.de)*

1. Literatur

2. Ronald Eikenberg, David Wischnjak, Böse und billig: Hacking-Gadgets, Gefahr durch angriffslustige Hardware, c’t 18/2017, S. 62 und S. 64
3. Verena Ehrl, Elektronische Übeltäter, Rechtliche Aspekte im Zusammenhang mit Spionage- und Sabotage-Gadgets, c’t 18/2017, S. 78
4. Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20.5.2021 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung, der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck:

heise.de/s/N76o
5. BGH, Beschluss vom 8.4.2021, Az. 1 StR 78/21: heise.de/s/rmDJ
6. LAG Baden-Württemberg, Urteil vom 17.9.2020, Az. 17 Sa 8/20: heise.de/s/MXBL
7. BGH, Beschluss vom 13.5.2020, Az. 5 StR 614/19: heise.de/s/Zvpw