Legaler Einbruch – Pentesting

Schwarze Box

Legaler Einbruch: So kann ein Pentest aussehen

Schwarze Box

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende klingen mag – Penetrationstests sind seit Jahren ein etabliertes Mittel, die Sicherheit von Systemen und Netzwerken zu überprüfen. Im Folgenden erfahren Sie, wie ein sogenannter Bl…

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende klingen mag – Penetrationstests sind seit Jahren ein etabliertes Mittel, die Sicherheit von Systemen und Netzwerken

zu überprüfen. Im Folgenden erfahren Sie, wie ein sogenannter Black-Box-Test abläuft.

Von Michael Wiesner

kompakt

- Pentester sind vom Betreiber eines Netzwerks beauftragte Hacker.
- Sie nutzen dieselben Werkzeuge wie echte Angreifer und decken Schwachstellen auf.
- Lediglich ausgestattet mit der Domain will Michael Wiesner in die internen Systeme seines Auftraggebers einbrechen.

Es ist April 2022, ich will eigentlich gerade den Laptop zuklappen, da flattert eine Anfrage in mein Postfach. Ein mittelständisches Maschinenbauunternehmen aus dem Norden Deutschlands will mich für einen sogenannten Pentest buchen.

Ein Pentest kann vieles sein, das Spektrum reicht von Sicherheitsanalysen einzelner Applikationen oder Systeme bis hin zur Simulation zielgerichteter Angriffe. Noch umfassender sind sogenannte „Red Team Assessments“. Dabei überprüfen Pentester, wie gut Systeme und Mitarbeiter zur Erkennung und Abwehr von Angriffsversuchen ausgerüstet sind.

Im Videotelefonat am nächsten Tag schildert der Chef der IT-Abteilung des Auftraggebers, worum es geht: Ich soll ohne Kenntnis über die IT-Infrastruktur in interne Systeme des Unternehmens einbrechen. Als einziger Anhaltspunkt dient die Domain – eine Information, die jeder Mensch mit Zugang zum Internet innerhalb von Sekunden herausfinden könnte. „Black-Box-Test“ nennt man solche Penetrationstests, bei denen der Pentester agiert wie ein typischer Angreifer. Alle weiteren benötigten Informationen muss ich dabei – in Abgrenzung zum White-Box-Test, bei dem der Pentester über Insiderwissen verfügt – selbst herausfinden. Der Einbruchsversuch soll einen zielgerichteten Angriff simulieren und möglichst verdeckt über

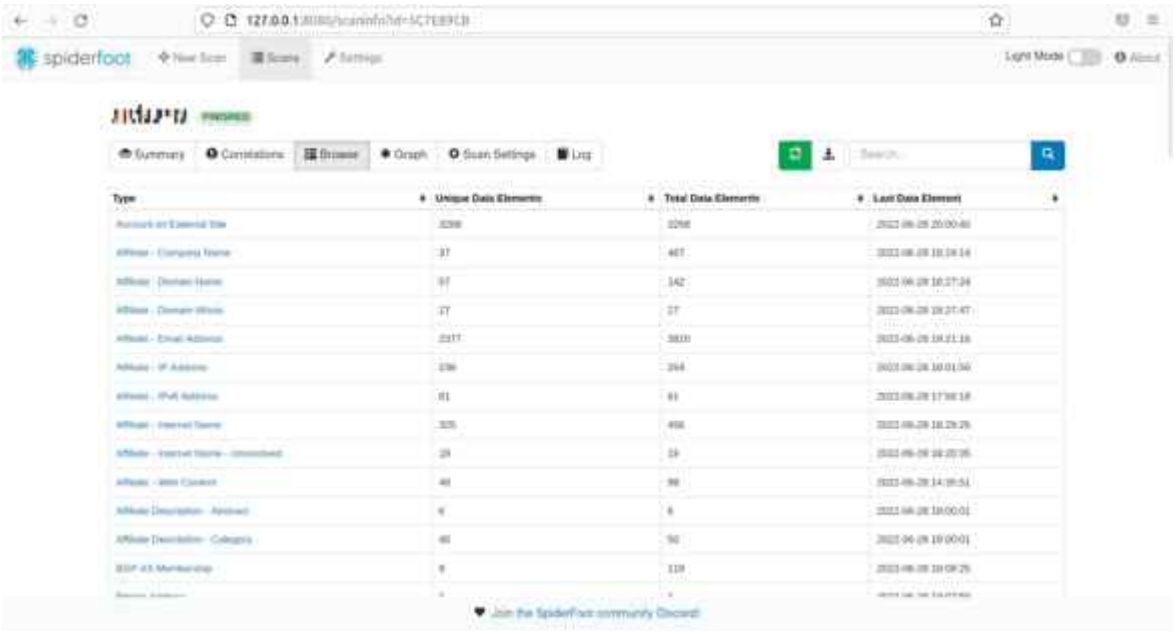
das Internet erfolgen. Entsprechend darf ich alle Mittel einsetzen, die auch ein echter Angreifer nutzen würde. Das könnte spannend werden – ich bin interessiert. Wir besprechen die Rahmenbedingungen und halten das Ganze vertraglich fest. In Angriff nehme ich den Test Anfang Juni.

Bei der Simulation eines solchen zielgerichteten Angriffs orientiere ich mich an den Phasen der MITRE ATT&CK Matrix. Darin werden die Taktiken und Techniken echter Cyberangriffe beschrieben und kategorisiert. Sie dient als Wissensdatenbank, die Verteidigern dabei hilft, Bedrohungen zu erkennen und abzuwehren, leistet mir bei einem Pentest, bei dem ich schließlich selbst in der Angreiferrolle stecke, aber ebenso gute Dienste.

Informationsbeschaffung

Ich starte mein Hacking-Vorhaben, indem ich alle frei verfügbaren Quellen nach Informationen über mein Ziel durchkämme. Dafür gibt es im Netz eine Reihe von Websites, Diensten und Datenbanken. „Open Source Intelligence“ (OSINT) nennt man diese Art der Informationsgewinnung auch (siehe c’t 16/2022, S. 138). Abfragen an WHOIS-Datenbanken und DNS-Server liefern mir erste Anhaltspunkte, mithilfe der Tools dnsrecon, spiderfoot und Shodan automatisiere ich einen Großteil der Arbeit. Das Python-Skript dnsrecon füttere ich im Bruteforce-Modus mit der Domain und einer Wortliste – es fragt Subdomains und Hostnamen ab und wertet praktischerweise anschließend gleich aus, welche IP-Adressen sich dahinter verbergen. Wie erwartet, liefert das Skript, und ich erhalte eine recht umfassende Liste der öffentlich erreichbaren Systeme meines Auftraggebers. Über die Kommandozeile rufe ich das OSINT-Tool Spiderfoot auf. Es nutzt eine größere Anzahl von Quellen für die Informationsgewinnung. Zum Beispiel ermittelt es mögliche Hostnamen auch durch die verwendeten TLS-Zertifikate. Auch liefert das Tool gültige Mailadressen, Telefonnummern, ähnliche oder verbundene IP-Adressen und Domains (siehe Bild

unten). Auch der Webdienst Shodan – sicher das prominenteste Beispiel für solche Scanner – liefert umfangreiche Informationen über die öffentlich erreichbaren Systeme meines Auftraggebers, die ich möglicherweise für den eigentlichen Angriff nutzen kann.



Spiderfoot ist ein OSINT-Tool, das dem Nutzer gleich eine ganze Palette an Informationen liefert, darunter auch Mailadressen.
Meine Zugriffe auf die öffentlichen Webseiten meines Auftraggebers werden zwar sehr sicher protokolliert, jedoch nicht blockiert, also kann ich davon ausgehen, dass sie nicht als schädlich erkannt werden. Zahlreiche Unternehmen, Organisationen und Einzelpersonen durchforsten das Internet laufend nach interessanten Systemen, Anwendungen oder Inhalten, sodass ein gewisses Grundrauschen besteht. Meine vorsichtig durchgeführten Verbindungsversuche gehen offenbar darin unter.

Vorsichtig anklopfen

Die gesammelten Daten verraten mir bereits eine ganze Menge über die Systeme und Anwendungen, die mein Auftraggeber verwendet, denn aus den DNS-Hostnamen kann ich ableiten, um welche Dienste es sich handelt: Bei „owa“ kann ich davon ausgehen, dass ein Exchange-Server betrieben wird und dieser

über „Outlook Web Access“ im Internet zur Verfügung gestellt wird. Generische Namen, wie „vpn“ oder „sslvpn“ sind selbsterklärend, „citrix“ weist auf ein Remote-Access-Gateway des gleichnamigen Herstellers hin. Teilweise sind die Hostnamen gleich, aber durchnummeriert – etwa owa2. Das könnte ein Hinweis darauf sein, dass mein Auftraggeber mehrere Versionen einer Anwendung einsetzt, oder darauf, dass ein Dienst über unterschiedliche Internetanbindungen bereitgestellt wird.

Die so gewonnenen Informationen über die Systeme und Dienste meines Auftraggebers sind noch nicht komplett. Aber um erste Angriffe zu starten, reichen sie aus. Für eine vollständigere Übersicht fehlt mir die Zeit – für den Penetrationstest sind lediglich sechs volle Arbeitstage veranschlagt – etwa zwei davon habe ich bereits für die Reconaissance-Phase, wie man die Phase der Informationsgewinnung im Fachjargon nennt – bereits aufgebracht. Für eine möglichst vollständige Übersicht muss man Ports scannen, beispielsweise mittels nmap oder einem Schwachstellenscanner wie Nessus oder OpenVAS. Die Herausforderung dabei ist, diese Scans so vorsichtig wie möglich durchzuführen, um weiterhin unentdeckt zu bleiben. Konkret bedeutet das, dass der Scan über einen langen Zeitraum verteilt werden muss, weil nur wenige gleichzeitige Verbindungen aufgebaut werden dürfen.

Da der vereinbarte Umfang und Zeithorizont des Penetrationstests kein solches Vorgehen erlaubt, wende ich die Holzhammermethode an: Über einen nur für diesen Vorgang genutzten Internetzugang starte ich ohne Rücksicht auf Verluste einen Portscan auf alle IP-Adressen und Ports. Dieser bleibt wegen des schon erwähnten Grundrauschens tatsächlich unbemerkt, liefert aber leider nicht die gewünschten Ergebnisse. Die „Portscan Protection“ der Firewall meines Auftraggebers blockiert den Scan erfolgreich. Das merke ich daran, dass mein Scan anfänglich zwar Ergebnisse liefert, die Systeme nach einer gewissen Zeit aber aufhören zu antworten.

Die Portscan Protection verlangsamt meine Verbindungsanfragen entweder stark oder blockiert sie ganz.

Für den Einstieg in die nächste Phase, die der Schwachstellenidentifikation, bleiben mir also nur die bereits gewonnen Informationen. „Schade“, denke ich – ganz so leicht scheint der norddeutsche Mittelständler es mir an dieser Stelle nicht zu machen.

Schwachstellensuche

Auch bei der Suche nach Schwachstellen greife ich auf Shodan zurück. Ich nutze den Webdienst, um auf Basis der Versionsnummern zu ermitteln, ob es bekannte Schwachstellen in den Diensten gibt. Leider ohne Treffer – laut Shodan hat nicht einer davon eine Schwachstelle, die ich für einen Angriff ausnutzen hätte können.

Ich muss wohl doch etwas genauer hinschauen: Mithilfe von Shodan, Spiderfoot und Dnsrecon habe ich knapp 70 offene Ports identifiziert. Das heißt, etwa 70 erreichbare Dienste warten darauf, genauer unter die Lupe genommen zu werden. Ich gehe systematisch vor. Zunächst filtere ich Dienste heraus, die nicht selbst betrieben werden und damit auch keinen potenziellen Zugriff auf die IT-Infrastruktur erlauben, wie etwa die Website beim Hoster. Die hebe ich mir für später auf, für den Fall, dass ich keinen direkten Weg in das Netzwerk meines Auftraggebers finden sollte. Die verbleibenden Portnummern geben Preis, um welche Art von Dienst es sich handelt. Um herauszufinden, welche Software und Version sich dahinter verbirgt, setze ich die Kommandozeilentools netcat oder alternativ telcat ein.

Zunächst surfe ich die identifizierten Webserver allerdings manuell über einen Webbrowser an, um zu erfahren, was sich hinter der URL tummelt. Dabei achte ich peinlich genau darauf, dass ich nicht nur die IP-Adresse, sondern auch den jeweilige Fully-Qualified Domain Name, kurz FQDN verwende. Dieser

vollständige Domainname einer Internetpräsenz ist eindeutig und er lässt sich den zum Nameserver gehörenden IPv4- oder IPv6-Adressen zuordnen. Das ist wichtig, weil oft mehrere unterschiedliche Webserver hinter der gleichen IP-Adresse betrieben werden – ohne die Angabe des FQDN würde ich möglicherweise nicht an die gewünschten Informationen kommen. Weil ich auf diese Weise – im Unterschied zum fehlgeschlagenen „Holzhammerscan" – nur noch einzelne Ports kontaktiere, könnte ich nun eigentlich umfangreiche Schwachstellenscans durchführen, ohne dass die Firewall wieder den Riegel vorschieben würde. Die Betonung liegt auf eigentlich – denn schon als ich die Websites manuell ansurfe, lande ich auf Login-Pages – ein deutlicher Hinweis darauf, dass mein Auftraggeber einen Reverse Proxy verwendet, um die Webseiten im Internet zu veröffentlichen. Das bedeutet, dass die Server nicht direkt angesprochen werden, sondern die Verbindungen vorab von einer Stellvertretersoftware angenommen werden. Schlimmer noch: Über die Eingabe bestimmter Parameter fingiere ich eine Directory-Traversal-Attacke und finde heraus, dass der Reverse Proxy zusätzlich über eine sogenannte Web Application Firewall verfügt. Das sind Systeme zur Erkennung und Abwehr von Angriffen, kurz WAF.

Das trübt meine Aussichten auf einen erfolgreichen Angriff über Sicherheitslücken in Web-Applikationen erheblich. Zähneknirschend verzichte ich auf einen umfangreichen Schwachstellenscan der Web-Apps – schließlich will ich die WAF nicht alarmieren. Ich verwende nikto und ein kommerzielles Tool namens Nessus, um die Websites auf Schwachstellen zu prüfen, werde jedoch nicht fündig. Komplett ertragslos verläuft meine Schwachstellensuche zum Glück trotzdem nicht. Beim manuellen Ansurfen haben Login-Pages mir verraten, dass es sich bei drei der Websites des Auftraggebers um Fernzugriffsportale handelt. Mithilfe von Nessus scanne ich sie ebenfalls auf Schwachstellen und gleiche zusätzlich die Versionsnummern mit der CVE-Datenbank https://cve.mitre.org ab. Leider fördert keine meiner Bemühungen eine

Sicherheitslücke in einem der Fernzugriffsportale zutage, aber ich nehme mir trotzdem vor, diese vorerst im Hinterkopf zu behalten.

Ein Schritt vor und zwei zurück

Die ernüchternde Zusammenfassung bis zu diesem Punkt: Keines der öffentlich erreichbaren Systeme des Auftraggebers besitzt offensichtliche Schwachstellen, die ich direkt zum Einbruch in die Systeme oder das Netzwerk hätte nutzen können. „Wäre ja auch zu leicht gewesen“, denke ich, während ich meine Optionen für das weitere Vorgehen abwäge. Ich habe nicht mehr viel Zeit, knapp zwei Drittel der maximal veranschlagten sechs Arbeitstage sind bereits verstrichen. Eine aufwendige Untersuchung der restlichen Webseiten, zum Beispiel mittels der beliebten Burp Suite fällt daher flach. Ein erneuter Blick auf die vereinbarte Leistungsbeschreibung zaubert mir dann aber doch ein Lächeln auf die Lippen. Fast hätte ich es vergessen, aber dort steht schwarz auf weiß, dass ich auch Phishingmethoden einsetzen darf. Phishing hat in der Regel das Ziel, den Empfänger dazu zu verleiten, Informationen preiszugeben oder ihn dazu zu bringen, Dateianhänge oder Links auf verseuchte Websites anzuklicken, über die dann Schadprogramme – sogenannte Remote-Access-Trojaner, kurz RAT – ausgeführt werden, die einen Zugang zum betroffenen System öffnen.

Spiderfoot hat mir während der Informationsbeschaffungsphase bereits eine Liste von circa 20 E-Mail-Adressen geliefert, denn auf der Webseite des Auftraggebers werden einige Mitarbeiter mitsamt der E-Mail-Adressen präsentiert. Das ist ein guter Start, aber ich würde die Angriffsfläche gerne vergrößern. Dabei spielen mir die beliebten Business Social Networks Xing und LinkedIn in die Hände. Anhand der Spiderfoot-Liste weiß ich ja bereits, wie die Unternehmens-Mailadressen aufgebaut sind und mit den Namen der Beschäftigten aus den Business-Netzwerken kann ich über ein

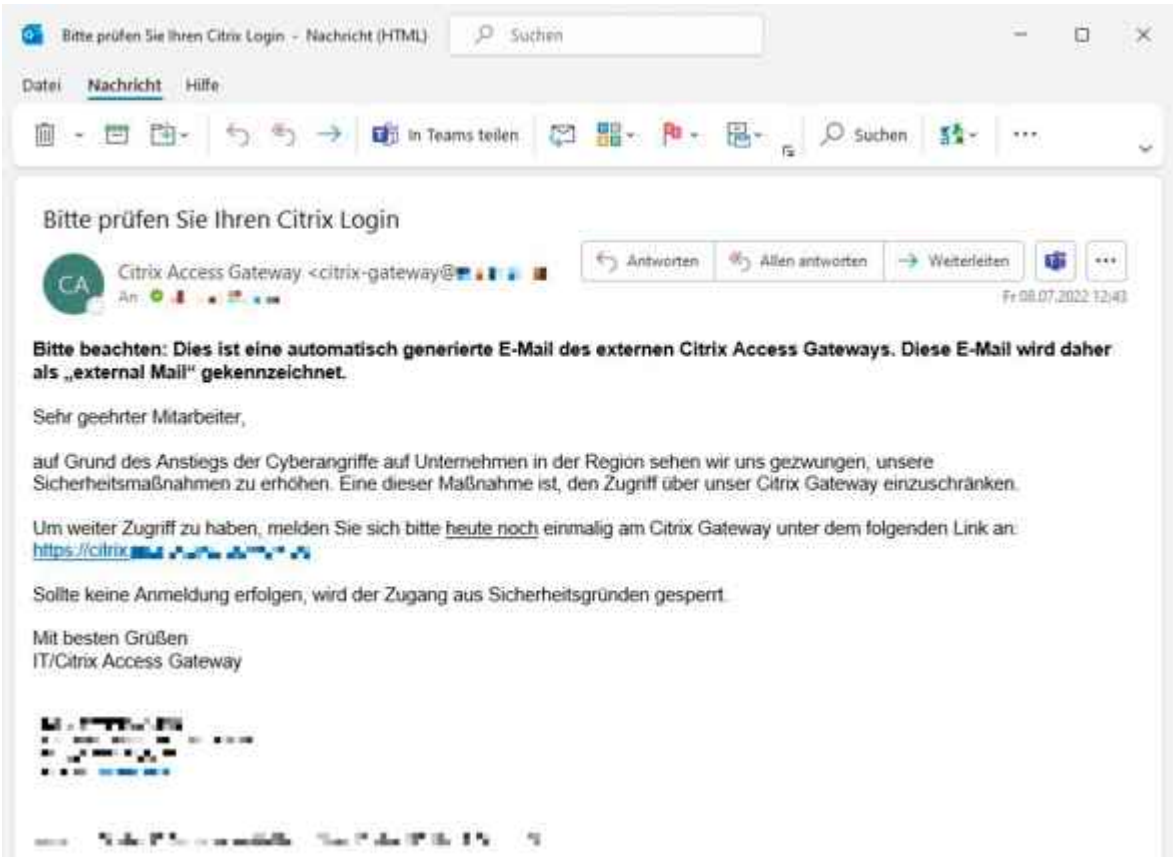
einfaches Skript leicht 50 weitere Mailadressen generieren.

Grundsätzlich sind solche Business-Portale ein Quell nützlicher Informationen. Über die eingetragenen Kenntnisse, Fähigkeiten oder die „ich biete“-Felder der Mitarbeiter lässt sich oft herausfinden, welche IT-Hersteller und Produkte eingesetzt werden. Dies ist besonders hilfreich, wenn die Hersteller von Firewalls, E-Mail-Gateways oder Endpoint-Security-Produkten genannt werden. Die Wahrscheinlichkeit ist hoch, dass diese dann auch in deren Unternehmen eingesetzt werden.

Eigene RATs zu erstellen, die nicht von der verwendeten Antivirussoftware erkannt werden, ist längst kein Hexenwerk mehr, so es sich denn um einen klassischen Virenschutz handelt. Ich versuche, den Trojaner über eine verschlüsselte Zip-Datei an der Firewall – beziehungsweise dem E-Mail-Security-Gateway – vorbeizuschmuggeln und erwarte fast, so mein Ziel zu erreichen, schließlich hat mich diese Methode in der Vergangenheit schon oft zum gewünschten Ziel geführt. Nicht jedoch bei diesem Penetrationstest. Mein Auftraggeber filtert sehr erfolgreiche alle E-Mails mit entsprechenden Dateianhängen heraus. Damit nicht genug – eine schnelle Recherche über den Webdienst mxToolbox zeigt, dass die absendende IP-Adresse bereits kurz nach den ersten Versuchen auf den bekannten Blacklisten landet. Leider führt auch das Einschleusen bösartiger Links für einen „Drive By Exploit“ nicht zum Ziel. Mir wird klar, dass ich es anders versuchen muss. Nur wie? – Die zuvor identifizierten drei Fernzugriffsportale kommen mir in den Sinn. Sie böten ideale Ansatzpunkte für eine Phishing-Kampagne, die auf das Abfischen von Zugangsdaten abzielt.

Ich mache mich an das Basteln einer weiteren Phishing-Mail. Sie soll so offiziell wie möglich aussehen – inklusive farblich passendem Layout und einer authentisch wirkenden Signatur. Von einer Wegwerf-Mailadresse frage ich höflich bei der jobs@-Mailadresse des Unternehmens an, an wen ich denn

meine Initiativbewerbung schicken könne. Wie erwartet, bekomme ich eine freundliche Antwort mit der gewünschten Information – und der Standardsignatur des Auftraggebers.



Mittels einer Phishing-Mail wird versucht, die Mitarbeiter des Auftraggebers auf eine Fake-Website zu locken.
Außerdem brauche ich eine Phishing-Webseite, in die mindestens eines meiner Opfer hoffentlich die Zugangsdaten eingeben wird. Gefälschte Webseiten bekannter Dienste, wie Microsoft Office 365, Facebook, Instagram oder Twitter lassen sich leicht über freie Tools wie zphisher erzeugen.

Zphisher erstellt Fake-Websites bekannter Dienste. Anpassen lassen sich diese aber leider nur bedingt.
In der Phishing-Mail müsste man dann nur noch auf die entsprechende Webadresse verweisen, um die eingegebenen Zugangsdaten anschließend abrufen zu können. Anpassungen, wie zum Beispiel das Logo meines Auftraggebers einzubinden, kann man daran aber leider nur bedingt vornehmen – für meine Zwecke kann ich zphisher deshalb leider nicht nutzen. Stattdessen erstelle ich manuell einen Klon von einem der verwendeten Fernzugriffsportale.

Eine geklonte Fake-Website soll die Phishing-Opfer dazu verleiten, ihre Zugangsdaten einzugeben.
Bleibt noch die Frage, auf welcher Adresse das gefakte Portal betrieben werden soll. Die Originaladresse lautet „citrix.DOMAIN.com“ – für meinen Klon verwende ich kurzerhand eine ähnlich aussehende Adresse: „citrix-DOMAIN.com“. Solche Doppelgänger-Domains sind auch bei realen Angreifern beliebt, da man auf den ersten Blick den Unterschied zwischen echten und gefälschten Adressen nicht erkennt.

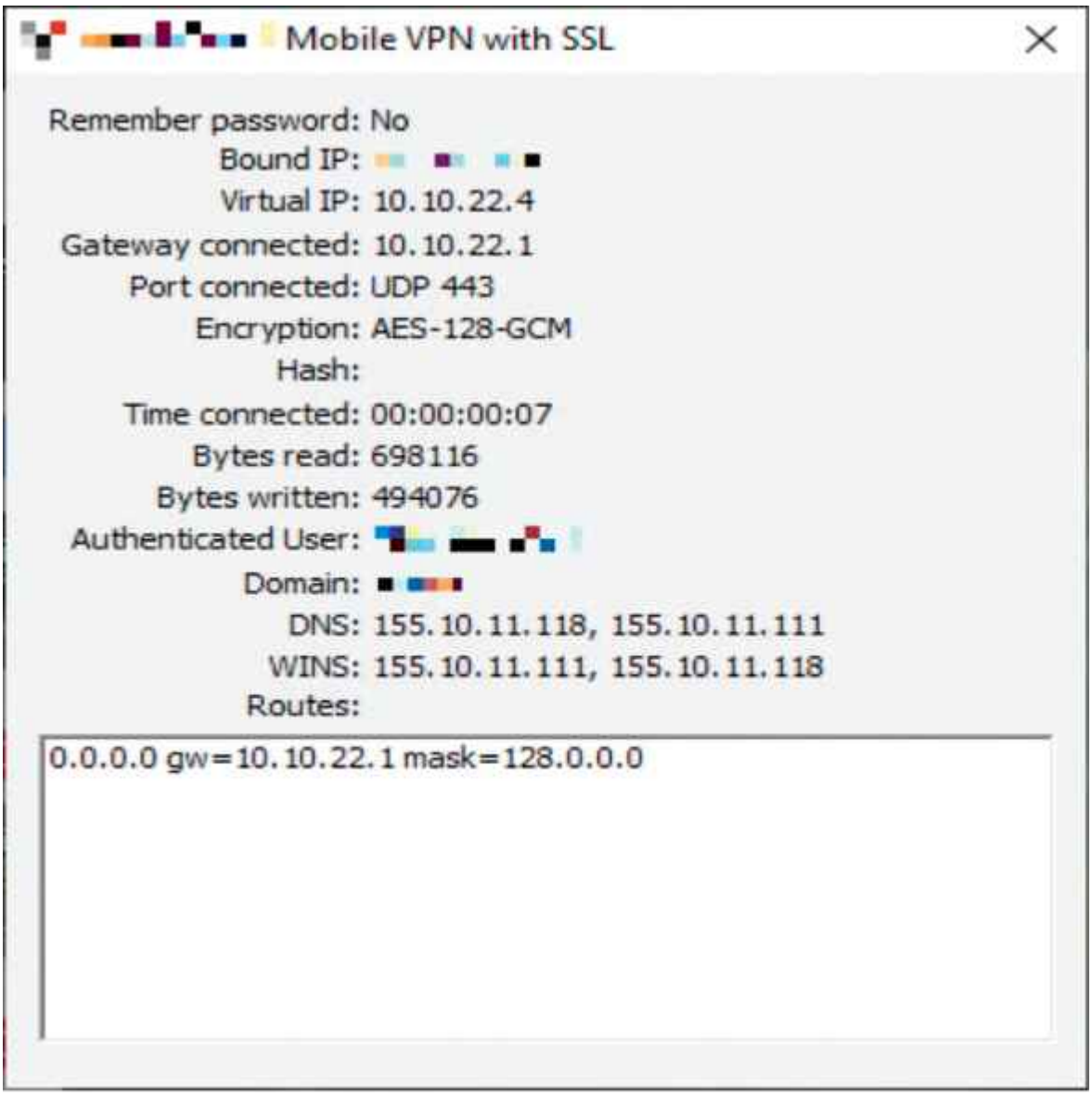
Bevor ich im großen Stil loslegen kann, gilt es vorab zu prüfen, ob die fingierte E-Mail die Empfänger überhaupt erreicht, oder ob sie – wie meine ersten beiden Versuche – durch Sicherheitssoftware blockiert wird. Ein Test mit ausgewählten Empfängern bringt die Ernüchterung: Das E-Mail-Gateway blockiert meine Phishing-Mails. Eine Überprüfung mittels mxToolbox verrät mir, dass meine IP erneut auf der Blacklist gelandet ist. Ich gerate ins Grübeln und ärgere mich zugegebenermaßen ein wenig, weil ich nicht gleich dahinter komme, warum. Die E-Mail war standardkonform, die IP-Adresse des Servers befand sich bis dato auf keiner Blacklist und auch der Text der E-Mail war nicht besonders spammy. Aber das E-Mail-Gateway ist anscheinend schlauer als gedacht: Ich vermute, es deklariert den eingebetteten Link auf die gefälschte Webseite als gefährlich, weil er Teile des Domainnamens des Auftraggebers enthält, jedoch nicht zu dessen

Servern gehört. Mir bleibt nur die Registrierung und Nutzung einer unverdächtigen Domain, die lediglich „citrix“ als Hostname aufführt und sonst möglichst offiziell aussieht. Ein Test mit dieser URL verläuft erfolgreich: Die E-Mails werden zugestellt. Anhand eintreffender Abwesenheitsnotizen kann ich zudem erkennen, dass die E-Mails nicht als Spam markiert wurden. „Feuer frei!“, denke ich grinsend.

Die eigentliche Phishing-Kampagne starte ich an einem Montag um 9 Uhr – pünktlich zum üblichen Arbeitsbeginn der Verwaltung. Und Bingo: Die ersten Zugangsdaten werden um 9:39 Uhr eingegeben. Jetzt darf ich keine Zeit verlieren. Wie klein mein Zeitfenster ist, kann ich nicht abschätzen, aber ich muss handeln, bevor es möglicherweise jemandem auffällt, dass Phishing-Mails im Umlauf sind und die Mitarbeiter – inklusive meiner Opfer – aufgefordert werden, ihre Zugangsdaten zu ändern.

Open the gates

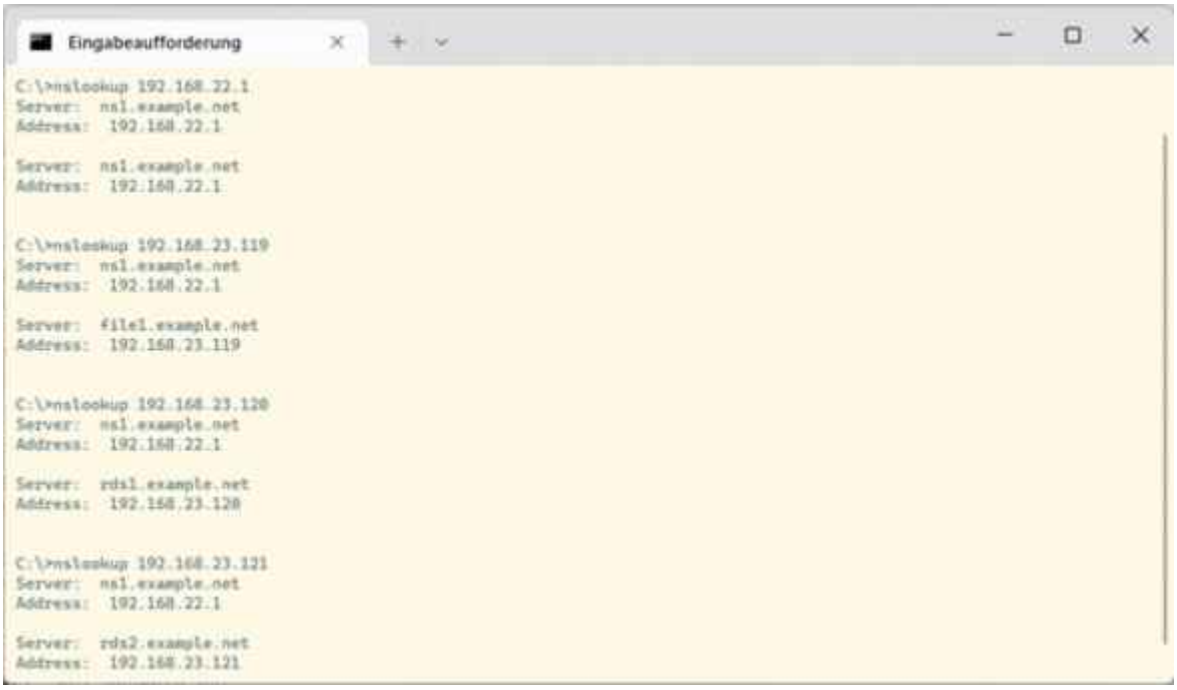
Meine Euphorie verfliegt, als die wirkliche Citrix-Anmeldeseite nach Eingabe der erbeuteten Zugangsdaten „Bitte Einmalpasswort eingeben“ meldet. Das Portal ist per Multi-Faktor-Authentifizierung abgesichert – und den zur Anmeldung benötigten zweiten Faktor besitzt nur der legitime Nutzer. Eins zeigt die Meldung jedoch: Die Zugangsdaten stimmen. Also versuche ich mein Glück beim nächsten Fernzugangsportal. Meine Hoffnung schwindet, als es ein Einmalpasswort anfordert. Aber ein Portal bleibt mir noch. Ohne große Hoffnung gebe ich die erbeuteten Zugangsdaten auch hier ein und halte die Luft an. Aber ich habe Glück: Nach dem Klick auf Enter zeigt mir das Portal einen Download-Link zum VPN-Dienst, den mein Auftraggeber verwendet. Ich installiere die Software, gebe die erbeuteten Zugangsdaten auch an dieser Stelle ein – und Bingo! – Der VPN-Client baut eine erfolgreiche Verbindung zum internen Netzwerk des Auftraggebers auf. Ich atme tief durch. Die nächsten Schritte muss ich sorgfältig planen.



Bingo! Das VPN-Gateway baut eine Verbindung zum internen Netzwerk auf.

Es gilt jetzt, das interne Netzwerk zu erkunden, um interessante Systeme und Daten zu identifizieren. Die Gefahr, erkannt zu werden, steigt dabei mit der Aggressivität des Vorgehens und den verwendeten Tools. Werden in dieser Phase Schwachstellenscanner oder Angriffswerkezuge, wie zum Beispiel Metasploit eingesetzt, ist die Gefahr groß, dass Endpoint-Security-Systeme oder vorhandene Intrusion-Detection-Systeme im Netzwerk dies erkennen, melden und anschließend die Verbindung zum internen Netzwerk getrennt wird. Unfehlbar sind solche Sicherheitsvorrichtungen allerdings nicht. Es ist möglich, sie auszutricksen, indem man sich als Angreifer verhält wie der eigentliche Anwender.

Aber ich will zuerst die wichtigste Frage klären – und dafür brauche ich sowieso noch keine Tools: Handelt es sich bei den VPN-Zugangsdaten auch um die Windows-Zugangsdaten? Klarheit verschafft mir die Anmeldung am Netlogon-Verzeichnis des Domain-Controllers. Es enthält in der Regel die Anmeldeskripte und kann daher auch von jedem Domain-Benutzer gelesen werden. Die Anmeldung funktioniert – ich habe tatsächlich die Zugangsdaten der Windows-Domain erbeutet.



Das Tool nslookup findet nach Eindringen in das Netzwerk die Namen weiterer Server heraus.

Jetzt könnte ich über PowerShell-Skripte oder Tools wie BloodHound oder PingCastle das Netzwerk und die Windows-Domain nach Schwachstellen durchforsten (siehe ct.de/yhxe). Ich entscheide mich aber lieber für die vorsichtigere Variante und sehe mich erst einmal manuell um. Im gleichen Netzbereich wie die Domain-Controller befinden sich üblicherweise auch weitere Server, deren Namen man durch einen Reverse-Lookup mittels des Standard-Tools nslookup auflösen kann. Durch den Aufbau der Hostnamen kann ich Rückschlüsse auf weitere Server ziehen. „rds1“ verweist etwa auf den ersten Terminalserver (Remote Desktop Services); „file1“ auf den ersten Fileserver (vergleiche Bild auf Seite 116). Getreu dem Motto „wer nicht wagt, der nicht gewinnt“, versuche ich mich auf den ersten

Terminalserver einzuloggen – und habe Erfolg. Der Server präsentiert die Standard-Arbeitsumgebung des unglückseligen Benutzers, dessen Zugangsdaten ich abgefischt habe – mitsamt allen Applikationen. Ich habe kompletten Zugriff im Kontext des ausgespähten Benutzers, inklusive E-Mail, Dateiablage, ERP-Software und Microsoft-365-Diensten, wie Sharepoint Online und Teams. Zudem offenbart ein kleines blaues Doppelpfeil-Symbol in der System Tray, dass der Auftraggeber das Support-Werkzeug TeamViewer einsetzt. Es könnte mir als mögliche Hintertür dienen, falls der Angriff erkannt und das VPN-Gateway abgeschaltet wird. Ein Blick in den Task-Manager des Servers zeigt die laufenden Dienste einer marktführenden „Endpoint Detection and Response"-Software, kurz EDR. Mein vorsichtiges Vorgehen war also mehr als angebracht. Der Versuch, zwischengespeicherte Authentifizierungsdaten auszulesen, zum Beispiel mit dem beliebten Tool Mimikatz, hätte höchstwahrscheinlich dazu geführt, dass ich entdeckt und aus dem System ausgesperrt worden wäre.

Bei einem klassischen „Double Extortion"-Angriff von Cyberkriminellen würden diese nun beginnen, die gefundenen Dateien zu exfiltrieren, sich im Netzwerk weitere Berechtigungen zu verschaffen, möglicherweise die Datensicherung zu manipulieren und Daten zu verschlüsseln, um anschließend Löse- beziehungsweise Schweigegeld zu fordern. Die Exfiltration von Daten bleibt meistens unerkannt. Ich simuliere den Vorgang, indem ich mehrere Gigabyte Daten in ein Zip-Archiv packe und es anschließend auf einen Webserver im Internet hochlade. Wie erwartet, bleibt der Vorgang unbemerkt. Aus Zeitgründen muss ich auf eine weitere Eskalation der Berechtigung verzichten – möglicherweise wird es dafür einen weiteren Penetrationstest geben.

Nachklang

Ich rufe meinen Auftraggeber an und informiere ihn mündlich über die gravierendsten Sicherheitslücken. Er zeigt sich

ernüchtert vom Resultat meines Penetrationstests. Weil ich keine Angriffswerkzeuge oder Schadsoftware eingesetzt habe, waren die im Unternehmen eingesetzten Sicherheitslösungen gegen meinen Angriff schlussendlich wirkungslos. Am Ende war es – wie so oft – menschliches Versagen, das mir ein Einfallstor in die geschützte Infrastruktur meines Auftraggebers eröffnete. Mehrere Mitarbeiter fielen auf meine Phishing-Attacke herein und die fehlende Multi-Faktor-Authentifizierung bei einem von drei Fernzugriffsportalen führte dazu, dass ich die erbeuteten Zugangsdaten tatsächlich nutzen konnte, um ins System einzubrechen. Eine alte Weisheit lautet „Der Angreifer muss nur einmal gewinnen, der Verteidiger immer“ – und dieser Black-Box-Test hat einmal öfter gezeigt, dass etwas Wahres dran ist.

Abgeschlossen ist die Geschichte an dieser Stelle allerdings weder für mich noch für meinen Auftraggeber. Zu meinen Aufgaben als Pentester gehört es auch, am Ende des Pentests einen aussagekräftigen Abschlussbericht zu erstellen. Notgedrungen setze ich mich wieder an den Schreibtisch und fasse die durchgeführten Schritte und die Ergebnisse des Black-Box-Tests zusammen. Ich beschreibe die entdeckten Schwachstellen genau und versuche, mich dabei möglichst verständlich auszudrücken. Das Ziel ist es schließlich, dass mein Auftraggeber die von mir entdeckten Schwachstellen versteht und sie beseitigen kann. *(kst@ct.de)*

Alle erwähnten und verwendeten Werkzeuge: ct.de/yhxe

Das sollte man bei der E-

Mail-Signatur beachten

entwickler.de – entwickler.de Deine Wissensplattform

[…]Weiterlesen…

Das sollte man bei der E-Mail-Signatur beachten

Mit freundlichen Grüßen …

von Michael Rohrlich

Auch wenn die „E-Mail-Unterschrift“ eine Art Schattendasein fristet – juristisch gibt es dabei einiges zu beachten.

Für die meisten Privatpersonen ist sie Platzhalter für Grußfloskeln, für Unternehmen stellt sie hingegen oftmals ein Marketinginstrument dar: die E-Mail-Signatur. Hierbei ist nicht die Rede von der digitalen Signatur – also dem Äquivalent zur händischen Unterschrift – die an Dateien oder eben auch an E-Mails angehängt werden kann, um eine rechtsverbindliche Erklärung abzugeben. Stattdessen geht es im folgenden Artikel um den textlichen Abschluss einer E-Mail, in deren Rahmen in aller Regel der Name des Absenders nebst etwaigen Zusatzangaben angegeben wird.

Ausgangssituation

Zwar ist es schon eine ganze Weile in Kraft und doch gibt es nach wie vor zahlreiche Verstöße gegen das Gesetz über elektronische Handels- und Genossenschaftsregister sowie das Unternehmensregister (EHUG) – und das jeden Tag. Denn mit dem Inkrafttreten des EHUG zum 01.01.2007 wurden zahlreiche

Gesetze geändert. Zwar ist die Realisierung der für alle kostenfreien Abrufbarkeit von veröffentlichungspflichtigen Unternehmensdaten wie Bilanzen oder Jahresabschlüsse im Internet (www.unternehmensregister.de) das primäre Ziel des EHUG. Allerdings wurden u. a. auch im Handelsgesetzbuch (HGB) diverse Normen neu hinzugefügt, die wiederum für unterschiedliche Unternehmensarten bestimmte Vorschriften enthalten. Unter anderem sind folgende Organisationsformen von Unternehmen betroffen:

- eingetragener Kaufmann (e. K./e. Kfr.)
- offene Handelsgesellschaft (oHG)
- Kommanditgesellschaft (KG)
- Gesellschaft mit beschränkter Haftung (GmbH)

Gegenüber Freiberuflern entfaltet das EHUG hingegen keine Wirkung, sodass sie von den verschiedenen Informationspflichten ausgenommen sind.

Exemplarisch sei an dieser Stelle die entscheidende Vorschrift für eine GmbH angeführt (§ 35a GmbHG):

„Angaben auf Geschäftsbriefen

(1) Auf allen Geschäftsbriefen gleichviel welcher Form, die an einen bestimmten Empfänger gerichtet werden, müssen die Rechtsform und der Sitz der Gesellschaft, das Registergericht des Sitzes der Gesellschaft und die Nummer, unter der die Gesellschaft in das Handelsregister eingetragen ist, sowie alle Geschäftsführer und, sofern die Gesellschaft einen Aufsichtsrat gebildet und dieser einen Vorsitzenden hat, der Vorsitzende des Aufsichtsrats mit dem Familiennamen und mindestens einem ausgeschriebenen Vornamen angegeben werden. Werden Angaben über das Kapital der Gesellschaft gemacht, so müssen in jedem Falle das Stammkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen angegeben werden.

(2) Der Angaben nach Absatz 1 Satz 1 bedarf es nicht bei

Mitteilungen oder Berichten, die im Rahmen einer bestehenden Geschäftsverbindung ergehen und für die üblicherweise Vordrucke verwendet werden, in denen lediglich die im Einzelfall erforderlichen besonderen Angaben eingefügt zu werden brauchen.

(3) Bestellscheine gelten als Geschäftsbriefe im Sinne des Absatzes 1. Absatz 2 ist auf sie nicht anzuwenden.

(4) Auf allen Geschäftsbriefen und Bestellscheinen, die von einer Zweigniederlassung einer Gesellschaft mit beschränkter Haftung mit Sitz im Ausland verwendet werden, müssen das Register, bei dem die Zweigniederlassung geführt wird, und die Nummer des Registereintrags angegeben werden; im Übrigen gelten die Vorschriften der Absätze 1 bis 3 für die Angaben bezüglich der Haupt- und der Zweigniederlassung, soweit nicht das ausländische Recht Abweichungen nötig macht. Befindet sich die ausländische Gesellschaft in Liquidation, so sind auch diese Tatsache sowie alle Liquidatoren anzugeben.“

Diese Regelung ist für ein Gesetz vergleichsweise klar formuliert und verdeutlicht auch dem juristischen Laien, was wobei anzugeben ist und wann Ausnahmen bestehen. Durch das EHUG wurden, wie § 35a GmbHG zeigt, vor allem auch neue Vorschriften im Hinblick auf bestimmte Pflichtinformationen in Geschäftsbriefen eingeführt. Als „Geschäftsbrief“ im Sinne des EHUG werden auch geschäftliche E-Mails eingestuft. Das EHUG basiert auf europäischem Recht, nämlich auf der Publizitätsrichtlinie und auf der Transparenzrichtlinie. Folglich gelten dem EHUG entsprechende Regelungen auch in den anderen Mitgliedsstaaten der Europäischen Union.

Informationspflichten

Die einzelnen Normen, die für die jeweiligen Gesellschaftsformen gelten, bestimmen alle in etwa das Gleiche wie § 35a GmbHG. Den betroffenen Unternehmen werden folgende Pflichtangaben abverlangt:

- Name des eingetragenen Kaufmanns/der eingetragenen Kauffrau bzw. Bezeichnung des Unternehmens inkl. Rechtsformzusatz
- Sitz des eingetragenen Kaufmanns/der eingetragenen Kauffrau bzw. des Unternehmens
- Vor- und Nachnamen des/der Vertretungsberechtigten (z. B. bei einer GmbH der/die Geschäftsführer, bei einer AG der/die Vorstandsvorsitzenden)
- Registerangaben (Registergericht und -nummer)
- bei Bestehen eines Aufsichtsrats zusätzlich die Vor- und Nachnamen des bzw. der Aufsichtsratsvorsitzenden
- wenn Angaben zum Stammkapital gemacht werden sollen, dann muss jedenfalls das Stammkapital aufgeführt werden (z. B. bei einer GmbH oder einer AG)

Über diese verpflichtenden Angaben hinaus können noch weitere Informationen in die E-Mail-Signatur eingebunden werden, zum Beispiel die vollständigen Kontaktdaten, Servicezeiten oder auch die Bankverbindung.

Praktische Umsetzung

Die aufgezeigten Pflichtinformationen sind auf jeden Fall in geschäftlichen E-Mails zu nennen. An welcher Stelle genau, dazu findet sich im Gesetz kein Anhaltspunkt. In aller Regel werden sie in einem für die E-Mail-Korrespondenz erstellten Briefbogen eingefügt oder eben im Rahmen der E-Mail-Signatur angegeben. Eine musterhaft formulierte, juristisch korrekte E-Mail-Signatur könnte so aussehen:

„Mustermann GmbH
Musterstr. 123
12345 Musterhausen
Geschäftsführer: Max Mustermann
Registerangaben: AG Musterhausen, HRB 12345“

In den meisten Fällen kommen zumindest noch die Kontaktdaten hinzu, wozu aber, wie gesagt, nach dem EHUG keine Pflicht

besteht. Alle darüber hinausgehenden Inhalte, insbesondere Werbung, sind hierbei tabu.

Die Pflichtangaben sind idealerweise als Text direkt in der E-Mail zu platzieren. Eine an die E-Mail gehängte „digitale Visitenkarte“ (z. B. VCF-Datei zur Einbindung in Outlook etc.) oder PDF-Datei sollte dagegen vermieden werden, denn dabei ist nicht gewährleistet, dass der Empfänger den E-Mail-Anhang öffnen und die darin enthaltenen Informationen auch zur Kenntnis nehmen kann.

Für etwaige Versäumnisse der Pflichten sind im EHUG generell vergleichsweise empfindliche Sanktionen vorgesehen. Die Höhe der drohenden Geldbuße kann bei 2 500 Euro und höher liegen. Zusätzlich sind – unter Umständen – im Hinblick auf fehlende Pflichtangaben in Geschäftskorrespondenz auch Abmahnungen der Konkurrenz oder von Verbraucherschutzorganisationen wegen eines Wettbewerbsverstoßes möglich.

Geschäftliche Korrespondenz

Letztlich stellt sich noch die Frage, was genau als Geschäftsbrief im Sinne des EHUG zu verstehen ist, denn heutzutage gibt es ja die unterschiedlichsten Formen von Korrespondenz, sowohl inhaltlich als auch in Bezug auf das Übermittlungsmedium. Nach der Vorstellung des Gesetzgebers sind gemäß EHUG alle Briefe, Faxe und E-Mails als Geschäftsbrief anzusehen, die an einen bestimmten, externen Empfänger gerichtet sind. Da möglichst viele geschäftliche Schreiben von den gesetzlichen Informationspflichten erfasst werden sollen, ist der Begriff „Geschäftsbrief“ im Zweifel sehr weit auszulegen, sodass die Eintrittshürde für das EHUG vergleichsweise gering ist.

Ausgenommen sind lediglich interne Kurzmitteilungen, Telefonnotizen oder sonstige Vermerke und vergleichbare Inhalte. Reine Werbeschreiben, die sich an einen nicht individuell bestimmten Personenkreis richten, sollen ebenfalls

nicht durch das EHUG erfasst werden.

Im Einzelfall kann es vorkommen, dass sich ein Schriftstück nicht eindeutig einstufen lässt. Im Zweifel gilt: lieber einmal zu viel Angaben geleistet, als einmal zu wenig.

Praxistipp

Unter den Begriff „Geschäftsbrief“ fallen nicht nur, aber insbesondere folgende Schreiben:

- Angebote
- Auftragsbestätigungen
- Empfangsbestätigungen
- Quittungen
- Rechnungen
- Mahnungen

Michael Rohrlich hat als Rechtsanwalt und Fachautor seinen Kanzleisitz in Würselen, Nähe Aachen. Seine beruflichen Schwerpunkte liegen auf dem Gebiet des Onlinerechts sowie des gewerblichen Rechtsschutzes. Weitere Infos zu den Themen aus den Rechtsbeiträgen sowie Gesetze und Gerichtsentscheidungen bietet er unter http://www.rechtssicher.info an.

Links & Literatur

[1] Homepage des Autors: http://www.ra-rohrlich.de

[2] Blog des Autors zum Thema Onlinerecht für Webmaster:

http://bit.ly/1W46GHD

[3] Blog des Autors zum Thema Onlinerechte von Verbrauchern: http://www.verbraucherrechte-online.de

[4] Weitergehende Infos zum Thema E-Commerce: http://bit.ly/1jAI1yt

[5] Videotrainings des Autors: http://bit.ly/1OI5ivc

CSR (Certificate Signing Request)

CSR (Certificate Signing Request)

Ein CSR (Certificate Signing Request), zu Deutsch Anforderung auf Ausstellung eines Zertifikats, ist eine speziell formatierte und verschlüsselte Nachricht. Die wird von einem Antragsteller für ein digitales SSL-Zertifikat (Secure Sockets Layer) an eine CA (Certificate Authority / Zertifizierungsstelle) gesendet. Der CSR bestätigt die Informationen, die eine CA benötigt, um das Zertifikat ausstellen zu können.

Ein PKI-System (Public Key Infrastructure) ermöglicht den sicheren Austausch von Daten über das Internet zwischen verifizierten Parteien. In so einem System muss vor der Bestellung und dem Kauf eines SSL-Zertifikats ein CSR erschaffen werden. Der Antragssteller muss zunächst ein

Schlüsselpaar generieren. Der Private Key (privater Schlüssel) dient zu Entschlüsselung der verschlüsselten Daten und der Generierung von digitalen Signaturen. Den Public Key (öffentlichen Schlüssel) benutzt man, um die Daten zu verschlüsseln und die Signaturen zu verifizieren. Sie müssen sowohl das Schlüsselpaar als auch den CSR auf dem Server erstellen, auf dem Sie das SSL-Zertifikat benutzen wollen. Das ist zwingend erforderlich, um die Integrität des Schlüsselpaars und der PKI im Allgemeinen zu garantieren.

Sobald das Schlüssel-Paar präpariert ist, kann der CSR generiert werden. Die CA wird all die notwendigen Daten des CSRs (siehe Tabelle) verwenden, um das Zertifikat auszustellen. Wie ein CSR generiert wird, hängt von der eingesetzten Webserver-Software ab. Sobald der CSR erstellt ist, kann man ihn bei der CA einreichen. Ist ein Antrag erfolgreich und für gültig erklärt, wird die CA das SSL-Zertifikat ausstellen und unterzeichnen.

Information	Beschreibung	Beispiel
Common Name	Der FQDN (Fully Qualified Domain Name) des entsprechenden Servers.	www.meinefirma.de mail.meinefirma.de *
Business Name / Organization	Der offizielle Name Ihres Unternehmens	Meine Firma, Mein Unternehmen
Department / Organization Name	Die Abteilung Ihres Unternehmens, die für das Zertifikat verantwortlich ist.	IT, Finanz-Abteilung
City / Town	Die Stadt, in der Ihre Firma den Sitz hat.	München, Hamburg

State & County / Region	Das Bundesland oder die Region, in der sich Ihre Firma befindet. Verwenden Sie hier keine Abkürzungen.	Bayern, Hessen
Country	Der zweistellige ISO-Code für das Land, in dem sich Ihr Unternehmen befindet.	DE, US
Email Address	Eine E-Mail-Adresse, um die Firma kontaktieren zu können.	admin@meinefirma.de zertifikate@meinefirma.de

** Generiert man einen CSR für ein so genanntes Wildcard-Zertifikat, sollte der Common Name mit einem * beginnen. Ein Beispiel wäre *.meinefirma.de*

Was ist ein SSL-Proxy?

Was ist ein SSL-Proxy?

Ein SSL-Proxy ist ein Gerät, normalerweise ein Router oder Computer, der den Datenverkehr von einem Client zu anderen Servern mithilfe des SSL-Protokolls (Secure Sockets Layer) weiterleitet. SSL ist ein verschlüsseltes Protokoll, das eine sichere Verbindung von einem Client zu einem anderen Client oder Server herstellt. SSL wird häufig in Verbindung mit dem Hypertext Transfer Protocol verwendet, um beim Surfen im

Internet eine sicherere Verbindung herzustellen. Das resultierende Protokoll oder die Sprache in einfacheren Ausdrücken wird als HTTPS bezeichnet.

Die Funktion eines Proxyservers besteht darin, den Datenverkehr für ein Netzwerk oder einen Client weiterzuleiten und zu filtern. In einem typischen Szenario gibt der Client, normalerweise ein Computer, eine Anforderung aus, in der Regel das World Wide Web zu besuchen, und der Proxy-Server empfängt diese Anforderung, filtert sie und leitet sie entsprechend weiter. Der Vorteil eines Proxyservers besteht darin, dass er den Netzwerkverkehr zentralisieren und gleichzeitig Sicherheit bieten kann.

Der Proxy kann Anfragen nach fast allen gewünschten Kriterien filtern. Wenn ein Unternehmen beispielsweise nur zu einer bestimmten Tageszeit zulassen möchte, dass der Datenverkehr aus dem Hauptnetz in ein anderes Netzwerk oder das World Wide Web geleitet wird, kann es den Proxyserver so einstellen, dass der gesamte Datenverkehr außerhalb des Netzwerks für den Rest des Netzwerks blockiert wird die Zeit. Da der Datenverkehr einen Server durchlief, konnte er auch für Nutzungsstatistiken überwacht werden. Eine hilfreiche Sache für viele Unternehmen.

Secure Sockets Layer (SSL) ist ein Protokoll, das Daten aus Sicherheitsgründen verschlüsselt. Zusätzlich zur Verschlüsselung wird auch ein System von Zertifikaten verwendet, mit denen andere Computer oder Server ihre Authentizität überprüfen. Das HTTPS-Protokoll, die Kombination aus HTTP und SSL, wird häufig zum Herstellen sicherer Verbindungen im Internet verwendet. Viele Unternehmen, die Kreditkarten online akzeptieren, verwenden beispielsweise das HTTPS-Protokoll, sodass niemand auf den Datenstrom zugreifen und vertrauliche Informationen abrufen kann.

Der Hauptzweck eines SSL-Proxys besteht darin, vertrauliche Daten in großem Umfang zu schützen. Es gibt viele Fälle, in denen dies wünschenswert wäre. Ein typisches Beispiel wäre ein

großes Unternehmen, das sensible Daten wie finanzielle oder rechtliche Informationen verarbeitet. Das Netzwerk könnte so eingerichtet werden, dass der gesamte ausgehende Datenverkehr des gesamten Unternehmens oder einer bestimmten Abteilung über einen SSL-Proxy geleitet wird. Dies kann zu einem zusätzlichen Schutz beim Senden von Informationen führen, insbesondere von Daten, die über das Internet übertragen werden müssen.

Eine andere typische Verwendung für einen SSL-Proxyserver wäre für Unternehmen, die Zahlungen in irgendeiner Form entgegennehmen. Oft haben sie einen Reverse-SSL-Proxy. Der Reverse-Proxy nimmt den eingehenden und nicht den ausgehenden Datenverkehr auf und kann das SSL-Protokoll intakt halten sowie das Innere des Netzwerks vor möglichen Eindringlingen schützen.

Was ist ein SSL-Proxy?

Was ist ein SSL-Proxy?

CMS / Blog per Proxy einbinden

CMS / Blog per Proxy einbinden

Unserer Erfahrung nach gelingt es einem Dritten in vielen Fällen über ein CMS oder Blog in einen Speicherplatz einzubrechen und Daten zu extrahieren oder Spam zu

verschicken.

Um die Sicherheit von Kundendaten zu erhöhen bieten wir ab einem eigenen Managed Server eine Proxy Lösung an, bei der z.B. ein Online Shop und ein CMS / Blog auf getrennten Speicherplätzen betrieben werden, aber den gleichen Domain Namen nutzen.

Ein Beispiel

Online Shop -> www.domain1-bei-profihost.com
Blog -> www.domain2-bei-profihost.com

Das Blog kann dann problemlos unter www.domain1-bei-profihost.com/blog eingebunden werden.

Der Clou ist:

Das Blog kann sogar problemlos bei einem externen Provider betrieben werden!

Auch ein für den Shop genutztes SSL Zertifikat für https://www.domain1-bei-profihost.com kann genutzt werden um Aufrufe des Blogs direkt mit zu verschlüsseln.

Für den Besucher ist nicht erkennbar, dass es sich um zwei getrennte Systeme handelt.

Sollte einem Dritten ein Einbruch in die Blog Software gelingen, hat er aber keinerlei Zugriff auf die Online Shop Daten.

Nutzen Sie die vorläufige Domain eines Speicherplatzes, brauchen Sie einen Workaround.

Damit die vorläufige Domain des getrennten Speicherplatzes keinen doppelten Content bei Suchmaschinen auslöst, nutzen Sie einen fiktiven Host, den wir für Sie nur im Betriebssystem kenntlich machen (als sog. statischen Host), hier im Beispiel:

internal-redirect.blogdomain-bei-profihost.de

Da auf allen Servern mit ServerCon bei uns das Webserver Modul mod_proxy aktiv ist, kann hier via .htaccess gearbeitet werden:

Ein Beispiel

```
RewriteEngine On
RewriteRule ^/?blog/(.*)$ https://blog.domain-bei-profihost.de/$1 [L,P]
```

Bei einer Subdomain sieht der Code so aus:

Ein Beispiel

```
RewriteEngine On
RewriteCond %{HTTP_HOST} ^blog\.domain-bei-profihost\.de$ [NC]
RewriteRule (.*) http://internal-redirect.blogdomain-bei-profihost.de/$1 [L,P]
```

Möchte man nur seine **Hauptdomain** mit und ohne „www.“, aber keine Subdomain via Proxy bedienen, legen Sie ein eigenes Verzeichnis im Wurzelverzeichnis des Speicherplatzes an.

Dann definieren Sie das Verzeichnis für die Hauptdomain im ServerCon Admin (Menüpunkte: Domain -> Hauptdomain und SSL / Let’s Encrypt) und legen eine .htaccess mit folgendem Code im neu erstellen Verzeichnis ab:

Ein Beispiel

```
DirectoryIndex disabled

RewriteEngine On

RewriteRule (.*) http://internal-redirect.blogdomain-bei-profihost.de/$1 [L,P]
```

Im Verzeichnis der getrennten „internal-redirect.blogdomain-bei-profihost.de“ leiten Sie via .htaccess dann alle Aufrufe auf das eigentliche Ziel um:

Ein Beispiel

```
<IfModule mod_rewrite.c>
RewriteEngine On

RewriteCond %{HTTP_HOST} !^blog\.domain-bei-profihost\.de$ [NC]
RewriteCond %{HTTP_HOST} !internal\.redirect\.cms-test\.de$ [NC]
RewriteRule (.*) https://blog.domain-bei-profihost.de/$1 [L,R=301]
</IfModule>
```

Allgemeine Informationspflichten für kommerzielle Websites

Allgemeine Informationspflichten für kommerzielle Websites

Eine Online-Shop-Betreiberin/ein Online-Shop-Betreiber muss neben der Informationspflichten, die nur zwischen Unternehmerinnen/Unternehmern und Verbraucherinnen/Verbrauchern zu beachten ist, auch allgemeine Informationen auf der Website zur Verfügung stellen. Diese Informationen müssen leicht und unmittelbar zugänglich sein und betreffen

- den Namen der Online-Shop-Betreiberin/des Online-Shop-Betreibers oder ihre/seine Firma,

- die geografische Anschrift, unter der das Unternehmen niedergelassen ist,
- Angaben, aufgrund deren die Nutzerinnen/Nutzer mit der Online-Shop-Betreiberin/dem Online-Shop-Betreiber rasch und unmittelbar in Verbindung treten können und ihre/seine E-Mail-Adresse,
- wenn vorhanden, die Firmenbuchnummer und das Firmenbuchgericht,
- wenn die Tätigkeit einer behördlichen Aufsicht unterliegt, die zuständige Aufsichtsbehörde,
- bei Online-Shop-Betreiberinnen/Online-Shop-Betreibern, die gewerbe- oder berufsrechtlichen Vorschriften unterliegen, die Kammer, den Berufsverband oder ähnliche Einrichtungen, der die Online-Shop-Betreiberin/der Online-Shop-Betreiber angehört,
- die Berufsbezeichnung und den Mitgliedstaat, in dem die Berufsbezeichnung verliehen worden ist,
- den Hinweis auf die anwendbaren gewerbe- oder berufsrechtlichen Vorschriften und auch einen Zugang zu diesen Vorschriften,
- wenn vorhanden, Umsatzsteuer-Identifikationsnummer,
- den Standort der Gewerbeberechtigung, wenn das Unternehmen nicht im Firmenbuch eingetragen ist.

Zusätzlich müssen Online-Shop-Betreiberinnen/Online-Shop-Betreiber, deren Unternehmen im Firmenbuch eingetragen ist, weitere Informationspflichten beachten. Diese finden sich unter Geschäftspapiere und Bestellscheine ebenfalls auf USP.gv.at.

Impressum und Offenlegung

Die Online-Shop-Betreiberin/der Online-Shop-Betreiber unterliegt der Offenlegungspflicht nach dem Mediengesetz. Diese reicht in ihrem Umfang weiter als ein Impressum. Die Impressumspflicht gilt für elektronische Medien, die wenigstens viermal im Kalenderjahr in vergleichbarer

Gestaltung verbreitet werden, z.B. elektronische Newsletter.

Hinweis

- Umgangssprachlich werden die Offenlegungspflichten nach dem Mediengesetz häufig als Impressum bezeichnet.
- Nähere Informationen zur „Impressumspflicht“ finden sich ebenfalls auf USP.gv.at. Die Wirtschaftskammer Österreich bietet Unternehmerinnen/Unternehmern auf Ihrer Homepage an, die gesetzlichen Auflagen durch Eintragung ihrer Firmendaten und Verlinkung darauf zu erfüllen.

Bei der Offenlegungspflicht wird zwischen „großen“ und „kleinen“ Websites unterschieden. Wenn eine Website keine über die Darstellung des persönlichen Lebensbereichs oder die Präsentation der Medieninhaberin/des Medieninhabers hinausgehenden Informationsgehalt aufweist, der geeignet ist, die öffentliche Meinungsbildung zu beeinflussen, handelt es sich um eine „kleine Website“. Die Offenlegungspflicht beschränkt sich in diesem Fall auf

- Name oder Firma der Medieninhaberin/des Medieninhabers,
- Unternehmensgegenstand,
- Wohnort oder Sitz (Niederlassung) der Medieninhaberin/des Medieninhabers.

Daher sind Websites, die sich auf die Präsentation des Unternehmens oder auf Produkte oder Dienstleistungen des Unternehmens beschränken, „kleine Websites“. Ein Online-Shop ohne redaktionelle Beiträge gilt somit als „kleine Website“.

Die Angaben zur Offenlegung können gemeinsam mit den allgemeinen Informationspflichten für kommerzielle Websites zur Verfügung gestellt werden. Ist die Medieninhaberin/der Medieninhaber mit der Online-Shop-Betreiberin/dem Online-Shop-Betreiber ident, muss nur der Unternehmensgegenstand offen gelegt werden, weil die weiteren Informationen bereits durch

die allgemeinen Informationspflichten für kommerzielle Websites abgedeckt werden.

Ein Online-Shop gilt als „große Website“, wenn auch redaktionelle bzw. meinungsbildende Beiträge auf der Website enthalten sind. Zu den oben genannten Offenlegungspflichten müssen für „große Websites“ zusätzlich folgende Angaben getätigt werden:

- Namen der vertretungsbefugten Organe der Medieninhaberin/des Medieninhabers (z.B. Geschäftsführerinnen/Geschäftsführer)
- Im Falle des Bestehens eines Aufsichtsrates auch dessen Mitglieder
- Für sämtliche der an einer Medieninhaberin/einem Medieninhaber direkt oder indirekt beteiligten Personen die jeweiligen Eigentums-, Beteiligungs-, Anteils- und Stimmrechtsverhältnisse
- Allfällige stille Beteiligungen an der Medieninhaberin/dem Medieninhaber
- Treuhandverhältnisse für jede Stufe
- Im Falle der Beteiligung von Stiftungen die Stifterin/der Stifter und die jeweiligen Begünstigten
- Im Falle eines Vereins der Vorstand und der Vereinszweck
- Erklärung über die grundlegende Richtung des Mediums bzw. der Website, die sogenannte Blattlinie

Nähere Informationen zur Offenlegungspflicht der „großen Website“ finden sich ebenfalls auf USP.gv.at. Zusätzliche Informationspflichten der Online-Shop-Betreiberin/des Online-Shop-Betreibers finden sich unter Informationspflichten ebenfalls auf USP.gv.at.

Neue Vorschriften für Online-Shops – Geoblocking-Verordnung

Seit 3. Dezember 2018 darf der Zugriff auf einen Online-Shop

wegen der Herkunft der Userin/des Users (Staatsangehörigkeit, gewöhnlicher Aufenthalt, Lieferadresse, IP-Adresse) nicht verweigert werden. Automatische Umleitungen sind nur dann erlaubt, wenn die Besucherin/der Besucher ihnen ausdrücklich zugestimmt hat, z.B. durch aktives Anklicken eines Feldes, und diese Auswahl jederzeit wieder aufgehoben werden kann.

Die Händlerin/der Händler darf jedoch das Liefergebiet selbst frei bestimmen und ist nicht verpflichtet, die Waren in jedes Land zu versenden. Das Liefergebiet sollte auf der Website klar erkenntlich gemacht werden.

Im Streitfall mit einer Verbraucherin/einem Verbraucher gilt der Gerichtsstand jenes Landes, auf das der Online-Shop ausgerichtet ist. Gibt es keine spezifische Ausrichtung auf ein einzelnes Land der Europäischen Union, gelten für eine österreichische Händlerin/einen österreichischen Händler das österreichische Recht und der österreichische Gerichtsstand.

Eine Unterscheidung bei Preisen aufgrund von Staatsangehörigkeit, Wohnsitz oder gewöhnlichem Aufenthalt ist verboten, außer es gibt dafür eine sachliche Rechtfertigung. Eine sachliche Rechtfertigung besteht etwa bei unterschiedlichen Umsatzsteuersätzen.

Auch bei den möglichen Zahlungsmitteln darf es grundsätzlich keine Unterscheidungen aufgrund von Staatsangehörigkeit, Wohnsitz oder gewöhnlichem Aufenthalt geben, außer es besteht eine sachliche Rechtfertigung.

Im Bereich zwischen zwei Unternehmen gelten diese Vorschriften nur, wenn die Käuferin/der Käufer keine Wiederverkäuferin/kein Wiederverkäufer ist.

Weiterführende Links

- Wirtschaftskammer Österreich (→ WKO)
- Website ECG– und mediengesetzkonform gestalten (→ WKO)

- Recht im Internet (→ onlinesicherheit.at)
- → NIC.at

Rechtsgrundlagen

- E-Commerce-Gesetz (ECG)
- Mediengesetz (MedienG)
- Gewerbeordnung (GewO)
- Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates vom 28. Februar 2018 über Maßnahmen gegen ungerechtfertigtes Geoblocking und andere Formen der Diskriminierung aufgrund der Staatsangehörigkeit, des Wohnsitzes oder des Ortes der Niederlassung des Kunden innerhalb des Binnenmarkts und zur Änderung der Verordnungen (EG) Nr. 2006/2004 und (EU) 2017/2394 sowie der Richtlinie 2009/22/EG

Letzte Aktualisierung: 16. Februar 2021

Für den Inhalt verantwortlich: Bundesministerium für Justiz

Social-Engineering-Angriffe auf Instagram-Accounts und wie Sie sich davor schützen

Instahack

Social-Engineering-Angriffe auf Instagram-Accounts und wie Sie sich davor schützen

Immer wieder kapern Phisher fremde Instagram-Accounts, um Profit daraus zu schlagen. So auch im Fall einer deutschen Olympiaschwimmerin, die sich Hilfe suchend an c’t wandte. Wir sind der Sache nachgegangen und stießen dabei auf weitere Fälle. Wir erklären, wie Sie Ihren Account schützen.

Von Ronald Eikenberg und Marie-Claire Koch

kompakt

- Instagram-Accounts, egal ob sehr populär oder nahezu unbekannt, sind ein lukratives Angriffsziel für Cyber-Kriminelle.
- Es ist wichtig, den Account mehrstufig abzusichern, wenn man nicht Gefahr laufen will, ihn für immer zu verlieren.
- Wer eine Mail erhält, die angeblich von Instagram stammt, sollte in der App kontrollieren, ob die Mail echt ist.

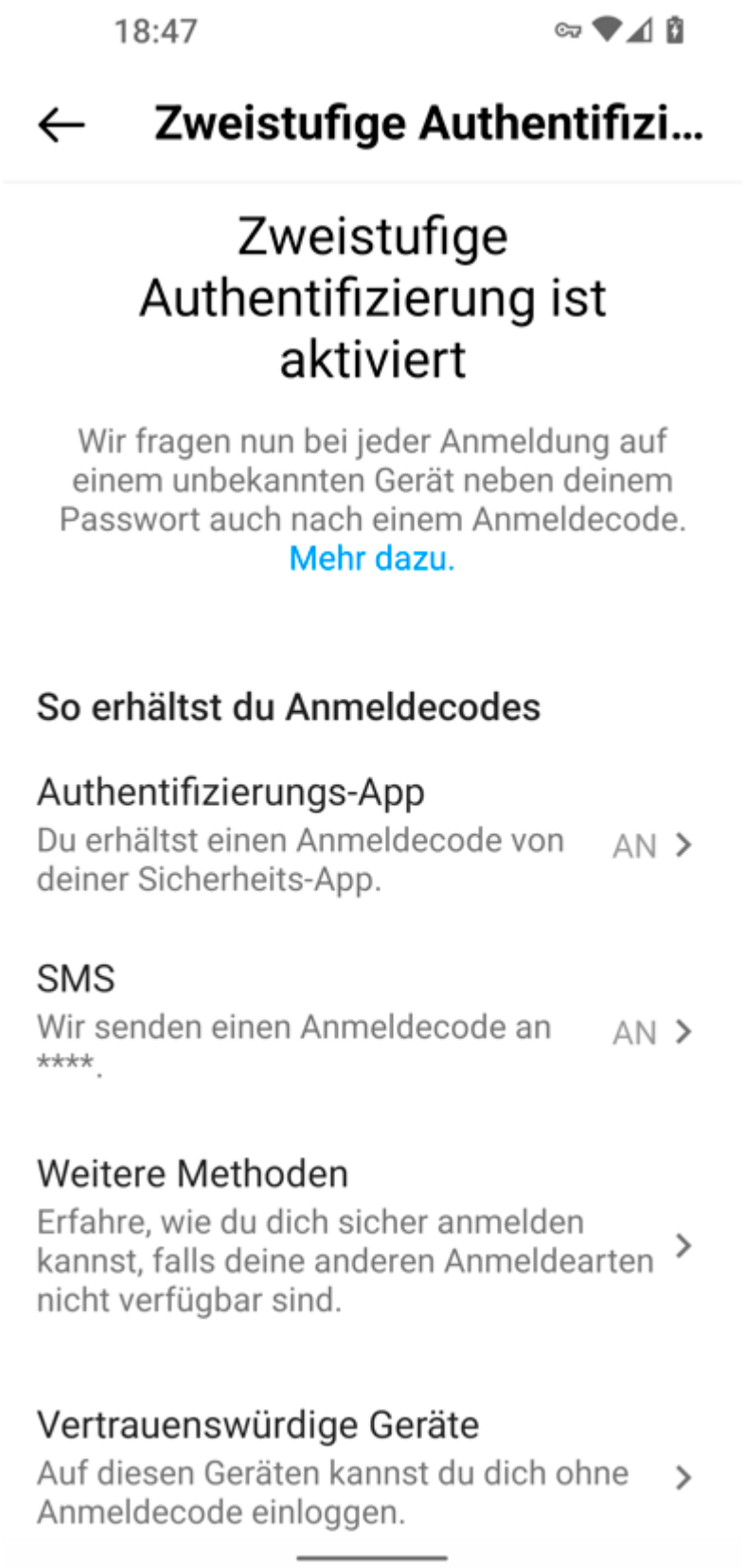
Phisher versuchen immer wieder an Zugangsdaten für Social-Media-Dienste wie Instagram zu kommen, um Accounts zu kapern und Profit daraus zu schlagen [1] – zum Beispiel durch Lösegeldforderungen oder dubiose Spam-Kampagnen. Dafür ist den Angreifern jeder Account gut genug, doch besonders hoch im Kurs stehen Instagram-Accounts, die der begehrte blaue Haken ziert. Er zeigt, dass es sich um ein durch Instagram verifiziertes Profil einer Person öffentlichen Interesses handelt. Aber auch mit nicht verifizierten Accounts können Phisher Geld machen, mangelndes öffentliches Interesse schützt Ihren Account daher nicht.

Der Instagram-Account einer Berliner Olympiaschwimmerin trägt diesen blauen Haken. Sie nutzt den Account, um mit ihren Fans in Kontakt zu bleiben und ihre Erfolge zu teilen – zum Beispiel ihre Teilnahme an den Olympischen Spielen in Tokio oder zuletzt an der Europameisterschaft in Rom. Vor einigen Monaten entdeckte auch ein Phisher die erfolgreiche Schwimmerin bei Instagram. Er kontaktierte sie über eine private Nachricht, gab sich als Instagram-Support aus, um sie in die Falle zu locken, und konnte letztlich die Kontrolle über ihren Account übernehmen.

Man spricht bei solchen Angriffen von Social Engineering, also der gezielten Manipulation des Opfers. Als die Schwimmerin bemerkte, wie ihr geschah, war das Kind bereits in den Brunnen gefallen. Der Angreifer hatte das Instagram-Konto bereits fest im Griff und die Account-Sprache auf Arabisch geändert. Die Schwimmerin wandte sich daraufhin an einen IT-Experten, der den Account jedoch auch nicht mehr retten konnte. Der Täter forderte unterdessen ein Lösegeld in Höhe von 150 Euro, zahlbar via PayPal.

Passwort: „Passwort“

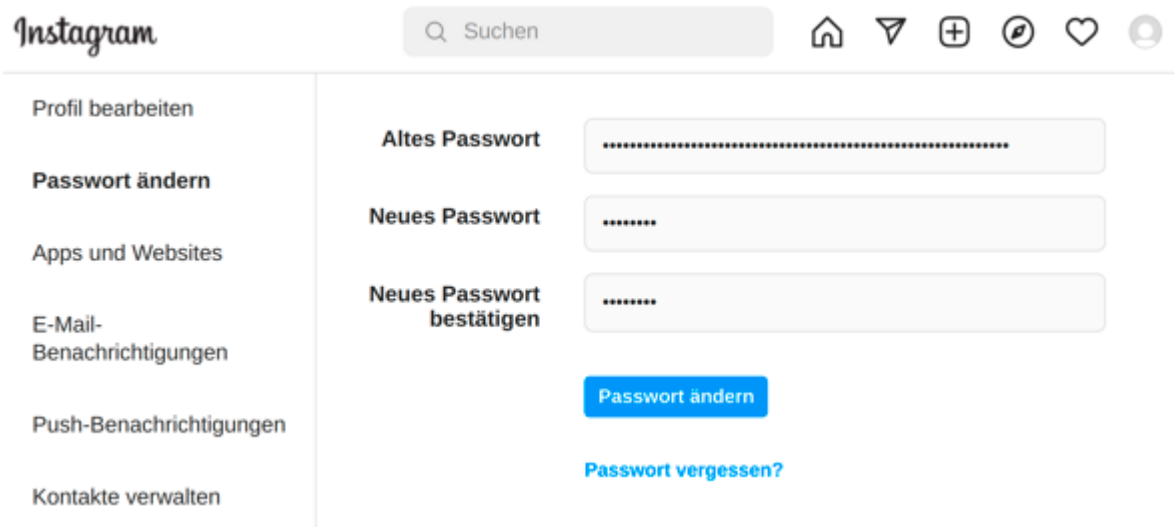
Statt der dreisten Lösegeldforderung nachzukommen, wandten sich die beiden an c’t. Im Rahmen unserer Recherche stießen wir auf drei weitere Sportlerinnen und Sportler aus dem Umfeld der Schwimmerin, deren Accounts ebenfalls gehackt waren. In zwei Fällen war ebenfalls Social Engineering im Spiel, im dritten wurde offenbar das Passwort erraten – es lautete schlicht „Passwort“. Alle betroffenen Accounts waren nicht nach Stand der Technik abgesichert: Die sogenannte Zwei-Faktor-Authentifizierung (2FA), die Angriffe auf Online-Accounts in den meisten Fällen vereiteln kann [2], war nicht eingeschaltet.



Wer einen Instagram-Account besitzt, sollte die zweistufige Authentifizierung einschalten.
Ist die 2FA aktiv, ist zumindest beim ersten Einloggen auf einem Gerät neben dem Passwort auch noch ein zweiter Faktor nötig. Das kann zum Beispiel ein kurzzeitig gültiger

Zahlencode sein, den man per SMS bekommt oder mit einer App wie dem Google Authenticator selbst generiert. Ein Hacker kommt in aller Regel nicht an SMS und erst recht nicht an das Geheimnis in der Authenticator-App. Mit einem erbeuteten Passwort kann er sich daher nicht einloggen.

Um die gehackten Instagram-Accounts der Athleten zu retten, kontaktierten wir die Pressestelle des Instagram-Betreibers Meta. Kurz darauf konnten die rechtmäßigen Account-Besitzer wieder auf ihre Konten zugreifen. Uns erreichen immer wieder ähnliche Zuschriften von Instagram-Nutzern, die Opfer von Cyber-Ganoven geworden sind. Weil wir nicht immer helfen können und damit es erst gar nicht so weit kommt, möchten wir Ihnen im Folgenden die wichtigsten Sicherheitstipps an die Hand geben, damit Sie Ihren Instagram-Account – oder die Accounts Ihrer Sprösslinge – angemessen absichern können.



Passwort: „Passwort“ – die Passwortanforderungen von Instagram sind eher locker, damit haben Cyber-Ganoven wie in diesem Fall dann leichtes Spiel.

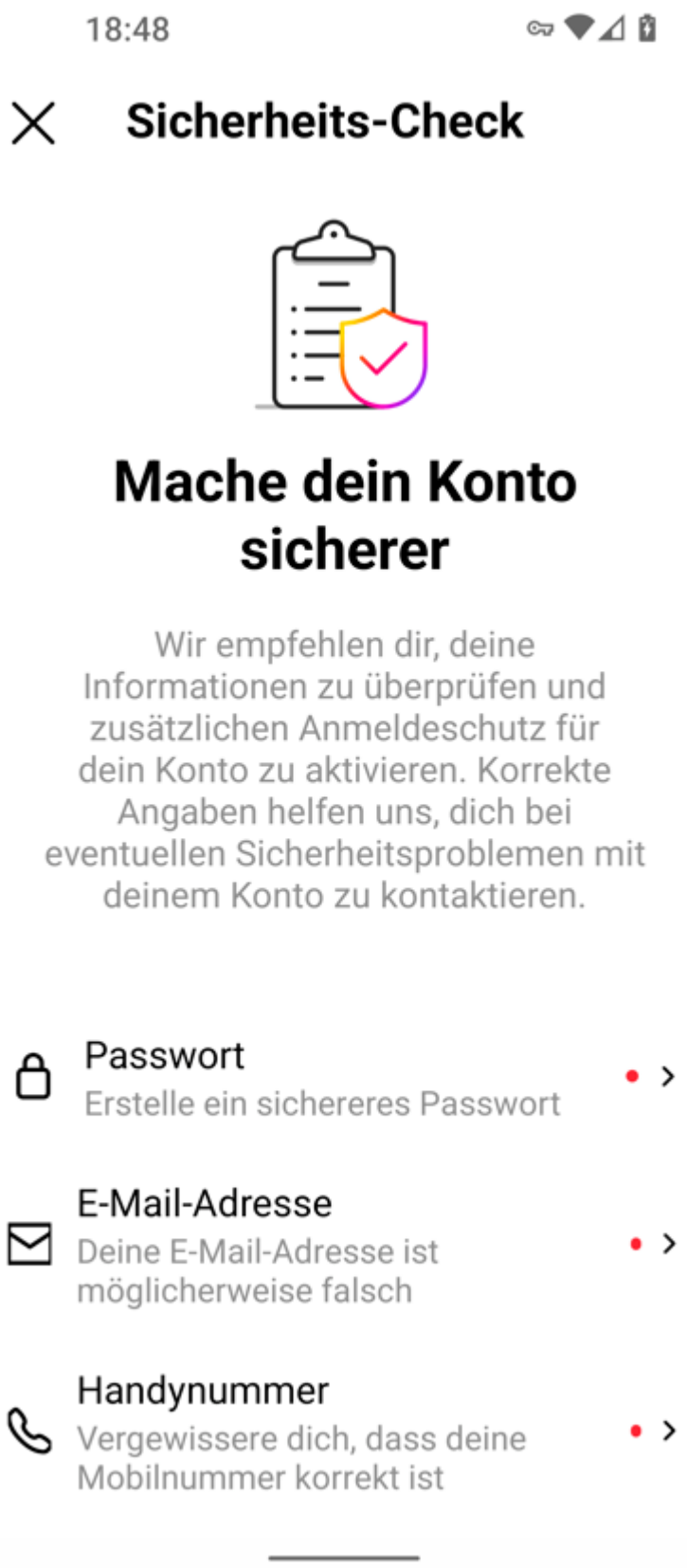
Instagram-Account absichern

Der beste Zeitpunkt, um sich um die Sicherheit Ihres Instagram-Accounts zu kümmern, ist genau jetzt, nicht später heute Abend oder am Wochenende. Sie müssen nur wenig Zeit investieren und ersparen sich früher oder später viel Ärger. Wenn Sie die von Instagram bereitgestellten Werkzeuge kennen

und nutzen, ziehen die meisten Angreifer unverrichteter Dinge zum nächsten Account weiter, der womöglich weniger gut abgesichert ist.

Den effektivsten Schutz gegen Phishing-Angriffe bietet die bereits erwähnte Zwei-Faktor-Authentifizierung (2FA), die Instagram „Zweistufige Authentifizierung“ nennt. In der Instagram-App aktivieren Sie den Schutz über den Menüknopf oben rechts und „Einstellungen/Sicherheit/Zweistufige Authentifizierung“, auf der Website klicken Sie in den Einstellungen auf „Privatsphäre und Sicherheit“, um die zweistufige Authentifizierung zu finden. Anschließend haben Sie die Wahl, ob Sie die zum Einloggen nötigen Zahlencodes per SMS zugeschickt bekommen möchten oder lieber selbst generieren wollen, mit einer Authenticator-App auf dem Smartphone.

Die SMS-Variante ist einfacher, aber auch unsicherer, weil es Angreifern gelingen kann, die SMS-Nachrichten mit den Codes abzufangen. Dennoch ist 2FA per SMS besser als nichts. Wir empfehlen die sicherere Variante „Authentifizierungs-App“, die sie jedoch nur mit der Instagram-App aktivieren können, nicht über die Website. Anschließend empfiehlt Ihnen Instagram geeignete Authenticator-Apps wie die von Google und erklärt Ihnen, wie Sie diese mit Ihrem Instagram-Account verknüpfen. Darüber hinaus sollten Sie ein langes Passwort für Ihren Account wählen, das nicht zu erraten ist und nur bei Instagram passt. Im besten Fall nutzen Sie einen Passwortmanager, um ein langes Zufallspasswort zu generieren und zu speichern.



Mit dem Sicherheits-Check überprüfen Sie die wichtigsten Security-Einstellungen bei Instagram.

Sicherheits-Check

Hilfreich ist der „Sicherheits-Check“, den Sie ebenfalls über die Sicherheitseinstellungen in der Instagram-App starten können. Diese Funktion macht auf gängige Sicherheitsprobleme wie ein schwaches Passwort aufmerksam und empfiehlt auch das Einschalten der 2FA, sofern sie nicht bereits aktiv ist. Zudem erinnert der Sicherheits-Check daran, dass man die Aktualität der hinterlegten Mailadresse und Telefonnummer kontrollieren sollte.

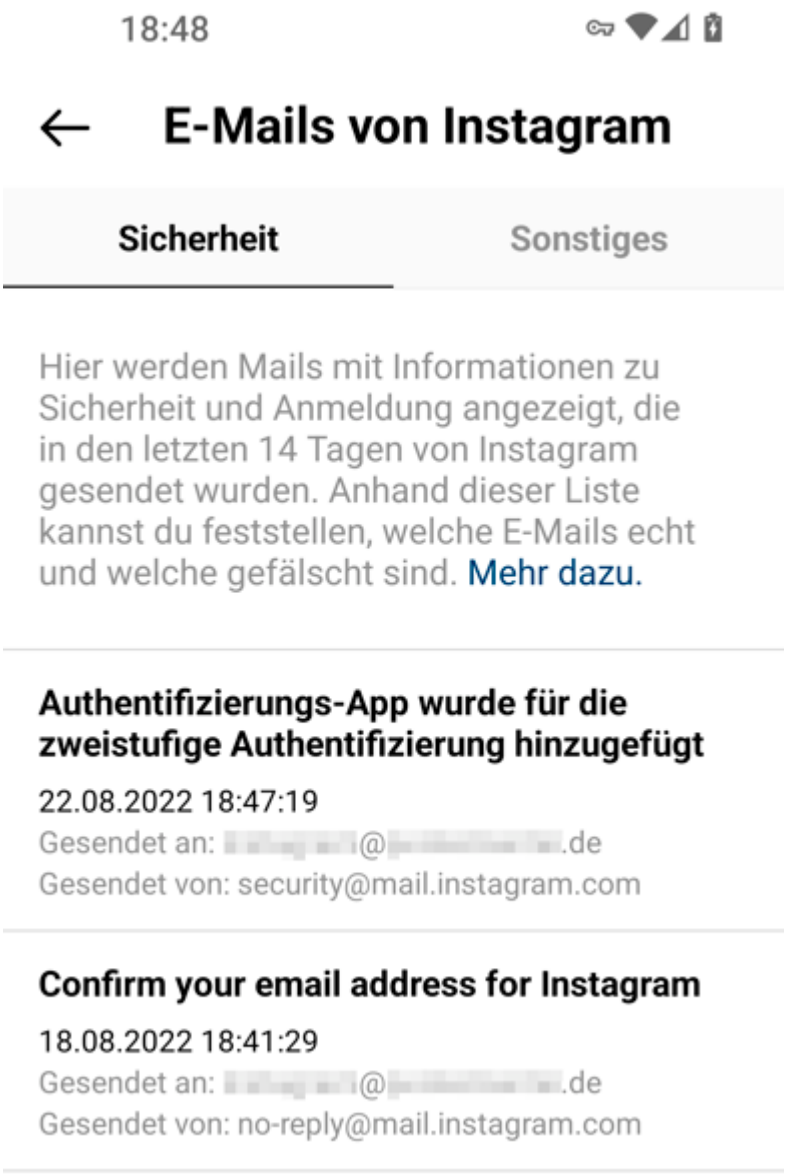
Wenn Sie Instagrams Betreiberfirma Meta diese Daten nicht anvertrauen möchten, funktionieren viele der Rettungsfunktionen von Instagram nicht, etwa weil das Unternehmen Ihnen im Fall der Fälle keinen Link zuschicken kann, über den Sie die Kontrolle über den gehackten Account zurückgewinnen können. Keine ganz leichte Abwägung, eventuell können Sie Instagram eine Zweit- oder Drittmailadresse zur Verfügung stellen – Hauptsache, Sie haben im Notfall sicher Zugriff darauf. Auch ein Profilfoto, auf dem Sie gut zu erkennen sind, kann die Rettung des Accounts erleichtern. Dazu gleich mehr.

Anti-Social-Engineering

Auch wenn Sie Ihren Account mit allen zur Verfügung stehenden Mitteln abgesichert haben: Technische Schutzmaßnahmen können Social Engineering nur erschweren, nicht verhindern. Angreifer hacken nicht Ihr Smartphone, sondern locken Sie trickreich in die Falle, etwa indem sie sich eben als Instagram-Support ausgeben und Sie mit einer plausibel klingenden Geschichte auffordern, Ihre Zugangsdaten auf einer externen Website einzugeben. Der zweite Faktor erschwert zwar einen solchen Phishing-Angriff, doch in jüngster Zeit fragen Online-Ganoven immer wieder auch nach dem temporären Einmalcode, mit dem sie den Account schließlich übernehmen können.

Allerdings können Sie sich vor dieser Form des Social

Engineering leicht schützen. Zunächst einmal sollten Sie sich darüber im Klaren sein, dass Sie Instagram niemals per Direktnachricht (Direct Message, DM) kontaktieren wird. Bei DMs ist Vorsicht geboten, auch wenn Sie den Absender kennen: Wurde ein Account gehackt, nehmen Angreifer schon mal Kontakt mit Freunden und Followern des Opfers auf, meist um die dazu zu bringen, eine gefährliche Website zu besuchen.



In der Instagram-App können Sie überprüfen, ob eine Mail, die angeblich von Instagram stammt, tatsächlich echt ist.

Mailcheck

Instagram kontaktiert Sie ausschließlich per Mail. Das wissen

allerdings auch die Cyber-Ganoven, sie verschicken täuschend echt aussehende Phishing-Mails im Instagram-Look. Wenn Sie eine Mail bekommen, die von Instagram stammen soll, sollten Sie sich also zunächst von der Echtheit überzeugen, bevor Sie die Mail ernst nehmen und auf einen Link aus der Nachricht klicken. Das ist bei Instagram erfreulich einfach: Öffnen Sie die Einstellungen in der App und tippen Sie auf „Sicherheit/E-Mails von Instagram“.

Dort listet die App alle Nachrichten auf, die Ihnen Instagram in den vergangenen 14 Tagen per Mail geschickt hat. Sie können die Nachrichten dort zwar nicht lesen, aber Sie erfahren Absender, Betreff und Sendedatum. Gleichen Sie diese Daten mit der Mail ab, um die Echtheit der Mail zu verifizieren. Der Absender sicherheitsrelevanter Instagram-Mails lautet stets security@mail.instagram.com. Wenn Sie auf Nummer sicher gehen wollen, dass der angegebene Absender nicht gefälscht ist, können Sie den Mail-Header inspizieren, wie in ct 19/2022 beschrieben [1].

Gehackten Account retten

Ist das Kind bereits in den Brunnen gefallen und Ihr Account wurde gehackt, dann müssen Sie schnell handeln. Je früher Sie aktiv werden, desto mehr Schaden können Sie abwenden. Nutzen Sie für sämtliche Rettungsversuche am besten ein Gerät, mit dem Sie bereits zuvor bei Instagram eingeloggt waren.

Beachten Sie die Mails von Instagram, um frühzeitig von einer Account-Übernahme zu erfahren. Der Dienst wird Sie über den Fremdlogin per Mail informieren und liefert Ihnen nicht nur den Zeitpunkt des Logins, Sie erfahren auch, welches Betriebssystem und welcher Browser mutmaßlich zum Einsatz kam. Zudem führt Instagram das Land an, aus dem die IP-Adresse des Nutzers stammt.

Auch wenn diese Daten nicht zu einhundert Prozent verlässlich sind: Sie eigenen sich gut, um darin Abweichungen zu Ihren

bisherigen Anmeldungen zu erkennen. Falls Ihnen bei der Kontrolle der Loginaktivität etwas komisch vorkommt, können Sie Ihren Account über den Link in der Mail („Sichere dein Konto hier“ oder „Secure your account here“) absichern. Achten Sie darauf, dass Sie auch tatsächlich auf https://www.instagram.com landen und nicht auf einer Phishing-Seite. Sie können über den Link ein neues Passwort setzen, das der Hacker nicht kennt. Überprüfen Sie von Zeit zu Zeit auch die „Login-Aktivität“ in den Sicherheitseinstellungen der App.

Informiert Sie Instagram ohne Ihr Zutun, dass Ihr Passwort oder die mit dem Account verknüpfte Mailadresse geändert wurde, sollten bei Ihnen die Alarmglocken läuten. Mit etwas Glück im Unglück können Sie aber auch in diesen Situationen die Kontrolle zurückgewinnen und die Änderung rückgängig machen, indem Sie in der Benachrichtigungsmail auf den Link „Sichere dein Konto hier“ klicken. Anschließend können Sie ein neues Passwort festlegen. Aber aufgepasst: Kontrollieren Sie auch in solch eiligen Fällen den Absender der Mail und das Ziel des Links genau, um sicherzustellen, dass es sich nicht um eine Phishing-Mail handelt. Geben Sie auf der verlinkten Seite nicht Ihr altes Instagram-Passwort ein.

Wurde der Account übernommen, kann ein Video-Selfie der letzte Ausweg sein.

Versteckter Rettungsweg

Für Härtefälle gibt es noch einen weiteren Rettungsweg über den Instagram-Support, der allerdings gut versteckt ist. Sie

erreichen ihn über die Instagram-App, indem Sie unterhalb des Login-Formulars auf „Erhalte Hilfe bei der Anmeldung“ tippen. Geben Sie oben Ihren Nutzernamen an und tippen Sie anschließend darunter auf „Du kannst dein Passwort nicht zurücksetzen?“. Die App fragt Sie daraufhin „Hast Du ein Foto von dir selbst in deinem Konto?“ – und das aus gutem Grund. Das Foto benötigt der Instagram-Support, um zu überprüfen, ob Sie der legitime Accountbesitzer sind. Falls Sie die Frage mit „Nein“ beantworten, ist Ihre Reise an dieser Stelle zu Ende und Sie landen im Hilfebereich.

Wenn Sie hingegen ein Foto in Ihrem Account haben und mit „Ja“ antworten, geht es weiter im Programm. Der genaue Ablauf variiert von Fall zu Fall. Instagram könnte Sie nach einem alten Passwort fragen und im darauffolgenden Schritt nach einem Bestätigungscode, den Sie sich an eine bei Instagram hinterlegte Mailadresse oder Handynummer schicken lassen können. Selbst wenn der Phisher die hinterlegten Daten geändert hat, stehen die Chancen gut, dass Sie hier noch Ihre wahre Rufnummer oder Mailadresse auswählen können und so an den Code kommen. Nach der Eingabe des Bestätigungscodes fragt Sie die App nach einer Mailadresse, über die Sie der Instagram-Support erreichen kann.

Video-Selfie

Haben Sie schließlich alle Hürden genommen, geht es ans Eingemachte: Die Instagram-App fordert Sie auf, Ihr Gesicht für ein sogenanntes Video-Selfie zu filmen. Im Rahmen dieses Vorgangs müssen Sie Ihren Kopf in vorgegebene Richtungen bewegen, um zu beweisen, dass Sie echt sind. Danach laden Sie das Video über den blauen „Senden“-Knopf hoch. Instagram beteuert, dass dieses Video maximal 30 Tage gespeichert wird und nicht zur Gesichtserkennung oder Speicherung biometrischer Merkmale genutzt wird. Wenn Sie das Video-Selfie hochgeladen haben, heißt es warten. Der Instagram-Support nimmt sich bis zu zwei Tage Zeit, um Ihr Anliegen zu bearbeiten.

Normalerweise geht es aber schneller. Nach der Überprüfung sendet Ihnen Instagram einen Link an die zuvor eingegebene Mailadresse, über den Sie ein neues Passwort festlegen können.

Falls Sie Ihren Facebook-Account mit Instagram verknüpft haben, gelten für diesen die gleichen Tipps: Nutzen Sie ein starkes Passwort, das nur bei Facebook passt, aktivieren Sie die Zwei-Faktor-Authentifizierung und achten Sie darauf, dass Ihre Kontaktdaten aktuell sind. Sie können zusätzlich die 2FA bei Instagram aktivieren, damit ein Angreifer, der bereits Kontrolle über Ihren Facebook-Account hat, nicht auch noch auf Ihr Instagram-Profil zugreifen kann.

Fazit

Instagram-Accounts stehen bei Cyber-Ganoven hoch im Kurs – insbesondere, aber nicht nur, wenn der begehrte blaue Haken das Profil ziert. Es ist daher wichtig, die Maschen der Angreifer zu kennen und frühzeitig geeignete Schutzmaßnahmen zu treffen. Wer sich nicht kümmert, riskiert sowohl, dass der Account gehackt wird, als auch, dass die vorhandenen Rettungsfunktionen ins Leere laufen, über die man die Kontrolle über einen gehackten Account zurückgewinnen könnte. *(rei@ct.de)*

1. Literatur
2. Ronald Eikenberg, E-Mails durchleuchtet, Phishing-Mails erkennen und abwehren, c’t 19/2022, S. 18
3. Niklas Dierking, Ronald Eikenberg, Schlosskombination, Verfahren und Geräte für sichere Online-Zugänge, c’t 9/2022, S. 18

Instagram-Hilfe zur Absicherung: ct.de/yqn6

Kartellamt: Google dominiert die Online-Werbe-Wertschöpfungskette

Kartellamt: Google dominiert die Online-Werbe-Wertschöpfungskette

Das Bundeskartellamt nimmt Google verstärkt ins Visier. Die Behörde erwägt in einem Bericht „breiter angelegte, möglicherweise strukturelle Eingriffe“, die über Einzelmaßnahmen hinausgehen.

Das 232 Seiten starke Diskussionspapier des Bundeskartellamts erklärt die verschiedenen Werbeformen und Geschäftsmodelle im

Detail.
Das Bundeskartellamt hat in einem Diskussionsbericht dargestellt, wie es den nicht an Suchmaschinen gebundenen Teil des Online-Werbemarktes einschätzt. Dabei handelt es sich zum Beispiel um die Banner, die viele Medienangebote (mit-)finanzieren. Allein in Deutschland werden laut dem Bericht pro Jahr vier bis fünf Milliarden Euro mit solcher Werbung umgesetzt. Dahinter stecke ein „hochkomplexes, für viele recht intransparentes System des automatisierten Handels mit Online-Werbeplätzen“, das der Bericht auf etlichen Seiten erklärt.

Im Rahmen der Untersuchung, so die Wettbewerbshüter, habe sich vor allem die Vormachtstellung Googles gezeigt: „Google ist auf nahezu allen Stufen der Wertschöpfungskette und bei praktisch allen relevanten Dienstleistungen vertreten und hat dabei in den meisten Fällen eine sehr starke Marktposition inne.“ Das Unternehmen kontrolliere wichtige Teile der nutzerseitigen Software-Infrastruktur wie den Browser Chrome und das mobile Betriebssystem Android. Damit bestimme es letztlich über die technischen Möglichkeiten mit, um Online-Werbung zu realisieren.

Der Bericht beurteilt nicht, ob Google seine Dominanz wettbewerbsschädigend ausnutzt, das Kartellamt will das aber weiter prüfen. Generell habe es neue Instrumente an die Hand bekommen, mit denen es gut gegen einzelne Praktiken vorgehen könne. Dazu zählt Andreas Mundt, der Präsident des Amts, den relativ neuen Paragrafen 19a des Gesetzes gegen Wettbewerbsbeschränkungen und den europäischen Digital Markets Act.

Bei Google könnte es aber nicht reichen, an einzelnen Stellschrauben zu drehen. Hier spricht der Bericht über „breiter angelegte, möglicherweise strukturelle Eingriffe“ – ohne diese weiter auszuführen. Das Bundeskartellamt ermöglicht es Marktteilnehmern und interessierten Kreisen, bis zum 28. Oktober 2022 Stellung zu dem Bericht zu beziehen. (jo@ct.de)

Podcasts bei YouTube und Twitter

YouTubeist bereits riesiger Anbieter von (Video-) Podcasts. Dieses Geschäft will die Plattform anscheinend weiter ausbauen, denn unter der URL youtube.com/podcasts **bietet YouTube gezielt Podcasts an**. Bis Redaktionsschluss war die Seite allerdings nur in den USA verfügbar; wann sie in Deutschland freigeschaltet wird, ist unklar.

Ebenfalls zunächst nur in den USA verfügbar ist eine neue Podcast-Funktion bei Twitter. Podcaster können ihre Sendungen dort veröffentlichen. Mit der Neugestaltung **führt Twitter personalisierte Hubs für Nutzer ein**, die sogenannten Stations. Sie gruppieren mehrere Inhalte auf Basis verschiedener Themen wie Nachrichten, Musik und Sport. (jo@ct.de)

Post: Digitaler Briefversand nun bei 1&1

Die Post kooperiert mit Web.de und GMX beim digitalen Briefversand. Inhaber eines E-Mail-Kontos bei den 1&1-Diensten GMX und Web.de können künftig Briefe digital aus einem neuen Online-Office heraus an die Deutsche Post übermitteln. Dort werden sie ausgedruckt, frankiert und auf dem Postweg als gedruckter Brief an die Empfängeradresse zugestellt. Der Dienst ist bis Jahresende für monatlich drei Briefe pro E-Mail-Konto gratis. Was er danach kosten wird, steht noch nicht fest.

Parallel zur Einführung des neuen Dienstes stellt die Deutsche Post ihren eigenen Service „E-Post“ für Privatkunden bis Ende November 2022 ein. Für Geschäftskunden werde E-Post als Plattform zur Digitalisierung der Briefkommunikation hingegen unverändert fortgeführt und weiter ausgebaut. (jo@ct.de)

Eine Rechtsverordnung soll Cookie-Abfragen eindämmen

Cookie-Banner adieu?

Eine Rechtsverordnung soll Cookie-Abfragen eindämmen

Die Bundesregierung will zentral verwaltete Cookie-Einstellungen ermöglichen. Nutzer könnten sogar pauschal alle Cookies ablehnen. Allerdings würden sie dann wohl mit Hinweisbannern zu kostenpflichtigen Angeboten überschwemmt.

Von Holger Bleich

Die Datenschutz-Grundverordnung (DSGVO) lässt derzeit keinen Ausweg: Website-Betreiber müssen ihre Besucher um Erlaubnis fragen, bevor sie Tracking- oder Analyse-Cookies auf deren Rechner setzen. Diese Einwilligung muss informiert erfolgen, weshalb nahezu jede werbefinanzierte Website Pop-up-Banner vorschaltet, die viel Text enthalten. Und viele Banner stupsen Nutzer mit Design-Tricks zum „Ja“.

Das im Dezember 2021 in Kraft getretene Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) sieht in seinem Paragrafen 26 einen deutschen Sonderweg vor, der die nervigen Banner überflüssig machen soll: In „anerkannten Diensten zur Einwilligungsverwaltung“ hinterlegen demnach Nutzer ihre Cookie-Präferenzen zentral. Websites fragen dann nicht mehr direkt den User, sondern holen sich Einwilligung oder Ablehnung bei dem Dienst ab [1].

Nun hat das von Volker Wissing (FDP) geführte

Bundesministerium für Digitales und Verkehr (BMDV) den Entwurf zu einer Verordnung erarbeitet, die den nach TTDSG erforderlichen Rechtsrahmen für die Einwilligungsdienste definieren soll. Nutzer können dem Entwurfstext zufolge „generelle Einwilligungen geordnet nach Kategorien für bestimmte Zugriffe auf Endeinrichtungen und Gruppen von Telemedienanbietern erteilen“. Die Dienste müssen gut erklären und informieren, außerdem sollen sie den Nutzer nicht mit Voreinstellungen beeinflussen.

Im BMDV glaubt man, im Entwurf die „richtige Balance“ zwischen den Interessen von Nutzern und kommerziellen Anbietern getroffen zu haben. Es gebe „keinen Anspruch auf kostenlosen Content“, war aus dem Ministerium zu hören. Diese Prämisse spiegelt sich im Entwurf wider: Zwar dürfen Nutzer im externen Einwilligungsdienst das Setzen von Cookies generell ablehnen. Doch gestattet es der Verordnungsentwurf Anbietern in diesem Fall, Nutzer mit vorgeschalteten Bannern darauf hinzuweisen, dass sie Tracking-Cookies benötigen, um die Site über Werbung zu finanzieren. Außerdem dürfen sie auf ein „kostenpflichtiges Alternativangebot“ (auf Medien-Websites die sogenannten „Pur-Abos“) verweisen oder den Nutzer „zur Änderung seiner Voreinstellungen beim Dienst zur Einwilligungsverwaltung“ auffordern.

Wie Websites die Nutzerpräferenzen beim Einwilligungsdienst abfragen sollen, lässt der Entwurf offen. In der Begründung zum Text, die c’t vorliegt, spricht das BMDV von „technikneutral“. Der Browser könne etwa einen HTTP-Request schicken, der die Zusatzinformation enthalte, dass der Endnutzer einen Dienst zur Einwilligungsverwaltung verwendet.

Auch wie die Dienste selbst funktionieren, will das BMDV dem Markt überlassen. Sie dürfen „kein wirtschaftliches Eigeninteresse“ daran haben, dass Nutzer möglichst viele Einwilligungen erteilen. Wohl aber dürfen sie kommerziell agieren und auch Geld für ihre Services verlangen. Sie müssen ein Sicherheitskonzept vorweisen und sich anschließend von der

Bundesdatenschutzbehörde prüfen und zertifizieren lassen.

Den ersten Entwurf hat das BMDV Ende August mit Bitte um Stellungnahmen an Wirtschaftsverbände geschickt. Er ist noch nicht mit anderen Bundesministerien abgestimmt. Bis er im Bundestag landet, werden noch viele Änderungen folgen – und Monate vergehen. Sollte der Bundestag die Rechtsverordnung durchwinken, muss die EU im sogenannten Notifizierungsverfahren prüfen, ob der Text europarechtskonform ist.

„Handwerkliche Fehler“

Daran regen sich bereits Zweifel. In einer ersten Stellungnahme kritisiert der Bundesverband Digitale Wirtschaft (BVDW) „handwerkliche Fehler“ im Text und moniert, dass der „aktuelle europäische Rechtsrahmen nicht hinreichend gewürdigt“ werde. Der Gesetzgeber habe „in den letzten Jahren zunehmend darauf hingewirkt“, die Einwilligung als Rechtsgrundlage für Datenverarbeitung zu forcieren, und nun wolle er „deren Einholung quasi untersagen“. Dies sei „aus Sicht der Datenökonomie und besonders aus Sicht der informationellen Selbstbestimmung der Nutzerinnen und Nutzer nicht der große Wurf, sondern ein großer Rückschritt“.

Das BMDV hat seinen Entwurf genau in einer Zeit vorgelegt, in der die EU dabei ist, ohnehin Cookie-Vorgaben und Einwilligungserfordernisse neu zu regeln: In Brüssel arbeiten Rat, EU-Parlament und Kommission gerade an einem Kompromiss zur E-Privacy-Verordnung. Weil diese EU-Verordnung über dem deutschen Recht stehen wird, könnte die deutsche Rechtsverordnung je nach Verhandlungsergebnis also schon in zwei bis drei Jahren wieder obsolet sein. (*hob@ct.de*)

1. Literatur
2. Holger Bleich, Löcher stopfen per Verordnung, Die bizarre Tracking-Regulierung in Deutschland, c’t 16/2022, S. 34

Microsoft schaltet Linux-Bootloader ab

Ausgebootet

Microsoft schaltet Linux-Bootloader ab

Dank Secure Boot starten Rechner nur noch Betriebssysteme, deren Bootloader von Microsoft signiert wurden. So sollen Rootkits und Bootviren keine Chance haben. Nun hat Microsoft etliche dieser Signaturen per Windows Update zurückgezogen und Linuxe so faktisch lahmgelegt. Wir erklären, wie Sie Ihr Linux trotz Microsofts Boot-Monopol wieder flott bekommen.

Von Mirko Dölle

Es erinnert an den Betriebssystemkrieg „Microsoft gegen Linux“ zur Jahrtausendwende: Mit dem Windows-Sicherheitsupdate vom 9. August hat Microsoft über 100 Linux-Bootloader auf die schwarze Liste gesetzt. Seither verhindert UEFI Secure Boot, dass etliche Linux-Distributionen booten. So konnten wir bei Redaktionsschluss das noch immer aktuelle Ubuntu 20.04 LTS und auch Manjaro Linux nicht mehr installieren – außer, man schaltet Secure Boot im BIOS-Setup ab. Auch Live-Linux-Systeme wie etwa Desinfec’t booteten nicht mehr auf PCs, bei denen zuvor das Windows-Update automatisch eingespielt wurde.

Das Update unter Windows wieder zurückzunehmen löst das Problem nicht, weil es den Inhalt des Flash-Speichers auf dem

Mainboard ändert, der auch den UEFI-BIOS-Code speichert. Kurzerhand Secure Boot abzuschalten kann das Problem bei manchen Computern sogar vergrößern und zu einem vollständigen Datenverlust unter Windows führen, sodass man am Ende ganz ohne funktionierendes Betriebssystem dasteht.

Laut Beschreibung von Microsoft dient das Update KB5012170 dazu, die Secure-Boot-Plattform zu stärken: UEFI Secure Boot überprüft vor jedem Start, ob der Bootloader des Betriebssystems korrekt mit dem Schlüssel einer vertrauenswürdigen Stelle signiert wurde. In der Praxis ist ab Werk nur ein solcher Schlüssel hinterlegt – nämlich der von Microsoft, damit das üblicherweise vorinstallierte Windows anstandslos bootet. Für Linux-Distributionen war Secure Boot anfangs ein rotes Tuch, schließlich waren der Linux-Bootloader Grub und die Linux-Kernel der Distributionen nicht von Microsoft signiert. Man musste Secure Boot erst ausschalten, um Linux installieren und benutzen zu können.

Praktisch alle Mainboard- und PC-Hersteller tragen im UEFI-BIOS als vertrauenswürdige Schlüssel nur die von Microsoft ein. Damit startet der Rechner ausschließlich von Microsoft signierte Bootloader, solange Secure Boot aktiviert bleibt.

Von Microsofts Gnaden

Die Lösung liefert der freie EFI-Loader Shim, der nur dazu gedacht ist, nach Überprüfung der Signatur den Linux-Bootloader Grub nachzuladen. Der Clou: Linux-Distributoren können ihren eigenen Signaturschlüssel in Shim hinterlegen und somit sicherstellen, dass etwa der in Ubuntu enthaltene Shim lediglich einen von Ubuntu signierten Grub und dieser wiederum einen von Ubuntu signierten Linux-Kernel nachlädt. Die distributionsspezifische Version von Shim lassen sich alle Linux-Distributoren bis heute von Microsoft für Secure Boot signieren, sodass Linux genau wie Windows anstandslos auf PCs mit aktiviertem Secure Boot starten sollte.

Allerdings wurden in den letzten zwei Jahren mehrere Bugs in Grub bekannt, mit denen Angreifer trotz Secure Boot unsignierten Code nachladen können. Microsoft hat darauf mit dem Update von 9. August reagiert und die Signaturen für die von den bekannten Sicherheitslücken betroffenen Linux-Bootloader zurückgezogen. Dazu wurde per Windows Update eine zusätzliche Revocation List mit den nun gesperrten Bootloader-Signaturen („Forbidden Signatures“, dbx) in den Flash-Speicher des UEFI-BIOS eingespielt.

Die Folge ist, dass sich zum Beispiel das noch bis 2025 gepflegte Ubuntu 20.04 LTS nicht mehr vom USB-Stick booten lässt – weder für Reparaturarbeiten noch für eine Neuinstallation. Ähnlich verhält es sich mit anderen Linux-Distributionen mit Langzeitunterstützung: Ältere Installationsmedien funktionieren nicht mehr. In den letzten Monaten aktualisierte Linux-Installationen auf Festplatte sollten hingegen einen neuen Bootloader erhalten haben, der nicht auf Microsofts Blacklist steht. Damit gibt es dann keine Bootprobleme. Auch der Installationsdatenträger von Ubuntu 22.04 LTS enthält einen neueren Bootloader mit noch gültiger Signatur und lässt sich deshalb uneingeschränkt verwenden.

BitAusLocker

Um eine lokale Linux-Installation trotz eines gesperrten Bootloaders starten zu können, damit man sie auf den aktuellen Stand bringen kann, müsste man Secure Boot im BIOS-Setup des Rechners deaktivieren. Doch das ist nicht ohne Risiken und Nebenwirkungen: Schaltet man Secure Boot später wieder ein und bootet Windows, wird man bei verschlüsselter Systempartition unter Umständen zur Eingabe des BitLocker-Wiederherstellungsschlüssels (Recovery Key) aufgefordert. Warum Windows nach Aus- und Wiedereinschalten von Secure Boot manchmal nach dem Wiederherstellungsschlüssel fragt, haben wir noch nicht herausfinden können, kennen das Phänomen aber sowohl aus eigener Praxis als auch von Leserzuschriften.

Sollten Sie unseren Rat aus [1] ignoriert haben und für die Anmeldung bei Windows ein Microsoft-Konto verwenden, hat Windows Ihren BitLocker-Schlüssel automatisch an Microsoft „zur sicheren Aufbewahrung“ geschickt – dann können Sie (und potenziell auch staatliche Stellen in den USA und anderswo) ihn in Ihrem Online-Profil abrufen und damit Ihre Windows-Partition entschlüsseln. Wer hingegen nur lokale Benutzerkonten verwendet, sollte den Recovery Key zuvor wie in [2] beschrieben abgerufen und notiert haben. Andernfalls, und falls Sie in Windows Home nur ein lokales Benutzerkonto angelegt haben, kommen Sie nicht mehr an Ihre Daten heran. Deshalb sollten insbesondere Windows-Home-Anwender die Geräteverschlüsselung in den Sicherheitseinstellungen von Windows deaktivieren und warten, bis die Entschlüsselung abgeschlossen ist, bevor Sie etwas an den Secure-Boot-Einstellungen Ihres Rechners verändern.

Zurück auf Los

Um Secure Boot nicht ausschalten und Probleme mit Windows riskieren zu müssen, können Sie die Schlüsselverwaltung von Secure Boot in Ihrem BIOS-Setup verwenden, etwa um ein nun

gesperrtes Linux für ein Update zu booten. Dazu sollten Sie zunächst über den Update-Verlauf unter Windows das Update KB5012170 entfernen, damit Sie es bei Bedarf zu einem späteren Zeitpunkt wieder einspielen können. Anschließend booten Sie neu und begeben sich ins BIOS-Setup Ihres Rechners, um dort die Änderungen des Windows-Updates wieder rückgängig zu machen.

Unter welchem Menüpunkt Sie die Schlüsselverwaltung für Secure Boot finden, ist nicht standardisiert. Manchmal ist sie in den Boot-Einstellungen versteckt, anderswo in den erweiterten Einstellungen oder Sie müssen erst in die Experten-Ansicht wechseln. Beim Asrock DeskMini versteckte sich der Menüpunkt „Secure Boot“ unter „Security“ im „Advanced Mode“ und wir mussten den „Secure Boot Mode“ erst auf „Custom“ umstellen, bevor wir das „Key Management“ aufrufen konnten.

Dort fanden wir unter „Forbidden Signatures“ (DBX) drei aktuell installierte Revocation Lists mit 77, 6 und 184 Einträgen. Die längste wurde im Rahmen des Updates KB5012170 eingespielt. Indem Sie auf „Delete“ klicken und nicht gleich sämtliche Einträge löschen lassen, gelangen Sie zur Auswahl der drei Listen und können gezielt die letzte entfernen. Anschließend speichern Sie die Änderungen im BIOS-Setup und können Linux wieder uneingeschränkt booten.

Mit dem Windows-Update vom 9. August wurde eine Liste zurückgezogener Bootloader-Signaturen mit insgesamt 184 Einträgen eingespielt. Indem Sie in der Schlüsselverwaltung des BIOS-Setup diese letzte Blacklist löschen, booten zuvor lahmgelegte Linux-Systeme wieder.

Microsofts Boot-Monopol

Da praktisch alle Hardware-Hersteller nur Microsofts Signaturschlüssel im UEFI-BIOS hinterlegen und Secure Boot seit Jahren auf allen PCs standardmäßig aktiviert ist, hat sich ein neues De-Facto-Monopol für den Software-Konzern aus Redmond ergeben. Mit dem Sicherheitsupdate vom 9. August hat Microsoft unfreiwillig demonstriert, welche Macht es dadurch besitzt: Letztlich entscheidet Microsoft, welche Betriebssysteme auf den Rechnern dieser Welt booten. Die Situation spitzt sich dadurch weiter zu, dass es den Herstellern inzwischen freigestellt ist, ob sie überhaupt noch eine Abschaltmöglichkeit für Secure Boot vorsehen.

Auf der Sicherheitskonferenz DefCon 30 kritisierten Jesse Michael und Mickey Shkatovur Microsofts Praxis, fremde Bootloader zu signieren: So gelang es ihnen mühelos, eine Signatur für den LOL-Bootloader („Laughing Out Loud“, „laut lachen“) zu bekommen, der beliebige, auch unsignierte Software

nachlädt. Das Fazit der Sicherheitsexperten: Secure Boot sei für Angreifer keine Hürde, mache aber Linux-Anwendern das Leben unnötig schwer.

Microsofts Boot-Monopol auf Rechnern praktisch aller Hersteller beweist, dass der freie Markt hier überfordert ist, wenn selbst Größen wie Red Hat, Suse oder Canonical von den Hardwareherstellern ignoriert werden. Deshalb ist es an der Zeit, dass der Gesetzgeber handelt: Man könnte etwa per EU-Einfuhrrichtlinie vorschreiben, dass Schlüssel entsprechend zertifizierter anderer Betriebssystemhersteller gleichberechtigt neben dem von Microsoft installiert werden müssen. So würden Anwender zumindest in Europa die Boot-Hoheit über ihre eigenen Rechner zurückgewinnen. *(mid@ct.de)*

1. Literatur
2. Axel Vahldiek, Zurück in die Kiste!, Windows ohne Microsoft-Konto nutzen, c’t 13/2021, S. 28
3. Jan Schüßler, Wohl oder übel, Keine Angst mehr vor Windows-Updates, c’t 8/2022, S. 148