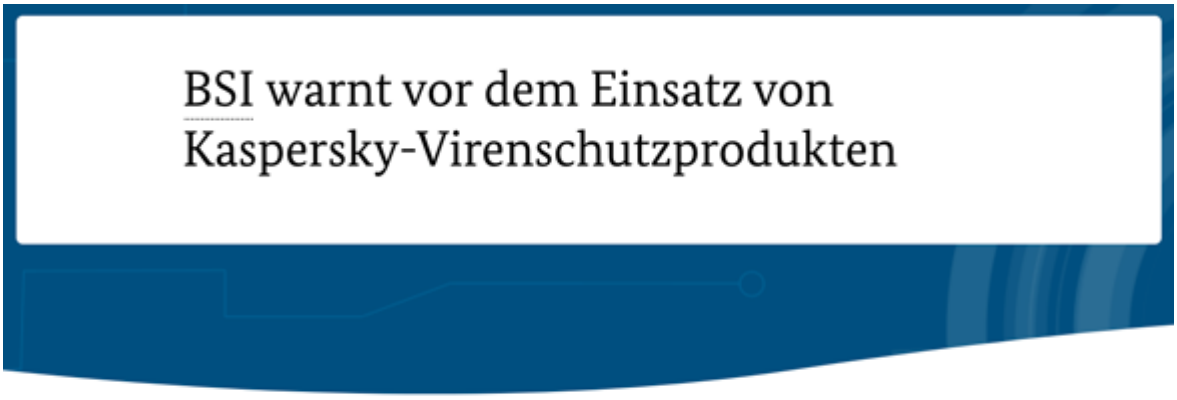
BSI-Warnung vor Kaspersky: Die Chronologie

BSI-Warnung vor Kaspersky: Die Chronologie

Interne Unterlagen beweisen, wie das BSI zusammen mit dem Bundesinnenministerium drei Wochen brauchte, um eine Warnung vor Kaspersky-Produkten auszusprechen.



Ort Bonn
Datum 15.03.2022

Erst am 15. März, rund drei Wochen nach dem Einmarsch Russlands in die Ukraine, veröffentlicht das BSI eine offizielle Empfehlung, keine weiteren Kaspersky-Produkte mehr zu benutzen.
Mitte März sprach das Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgrund des Angriffskrieges auf die Ukraine eine Warnung vor sämtlichen Kaspersky-Produkten aus. Grund: Kaspersky ist ein russischer Antivirenhersteller mit Sitz in Moskau. Daher besteht die realistische Gefahr, dass die russische Regierung die tiefreichenden Rechte ausnutzt, die Antivirenprogramme in Betriebssystemen haben, um beispielsweise an Informationen heranzukommen. 370 Seiten an Dokumenten zeigen nun die Chronologie dieser Entscheidung.

Der Bayerische Rundfunk forderte die Unterlagen durch eine Anfrage nach dem Informationsfreiheitsgesetz an und wertete sie zusammen mit dem Magazin Der Spiegel aus (siehe

ct.de/yu6a). Daraus geht hervor, dass das BSI kurz nach Beginn des Krieges recht schnell die brisante Lage Kaspersky erkannte und nach technischen Gründen suchte, um eine Warnung auszusprechen.

In den internen Mails diskutierten die BSI-Angestellten rege Argumente wie: „Es ist nicht sicher, dass Kaspersky noch die vollständige Kontrolle über seine Software und IT-Systeme hat bzw. diese nicht in Kürze verlieren wird.“ Und man müsse mit „feindlichen Übergriffen auf deutsche Institutionen, Unternehmen und IT-Infrastrukturen“ rechnen. Aber nicht alle waren dieser Meinung, ein Abteilungsleiter schrieb etwa, dass man nicht vorschnell handeln solle oder womöglich sogar rechtswidrig, denn immerhin habe Kaspersky schon vor längerer Zeit angefangen, Server in die Schweiz auszulagern.

Nach einer intensiven Debatte nickte der BSI-Chef Arne Schönbohm am 5. März intern eine mögliche Warnung ab. Es folgten mehrere Absprachen mit dem Bundesinnenministerium (BMI), dem das BSI unterstellt ist. Etwa zeitgleich wendete sich Kaspersky Hilfe suchend an das BSI und erhoffte sich Rückendeckung, was aber innerhalb der Behörde auf taube Ohren stieß.

Erst einen Tag vor dem Aussprechen der Warnung durch das BSI erfuhr Kaspersky per Mail von der Entscheidung, mit der Bitte zu Stellungnahme innerhalb von drei Stunden. Das Unternehmen fühlt sich nach eigener Aussage übergangen und diskreditiert, weswegen es rechtliche Schritte eingeleitet hat. In zwei Instanzen wurde dem BSI recht gegeben, eine abschließende Entscheidung fällt aber erst im langwierigen Hauptverfahren.

Nach dem Okay des BMI sollte die Warnung am 16. März veröffentlicht werden, doch die Presseabteilung grätschte dazwischen und wünschte sich die Erklärung einen Tag früher zu veröffentlichen: „Dann können wir damit in die nächste c’t und in Die Zeit hineinkommen und das BSI als Akteur positionieren.“ So ging die Warnung schließlich am 15. März

raus.

Laut den Dokumenten sollte ursprünglich die Sicherheitsfirma G Data mit in der Erklärung auftauchen, da die ehemalige Frau des Kaspersky-Chefs Natalja Kaspersky 17 Prozent des Unternehmens hält. Diese stehen laut Spiegel aber offenbar zum Verkauf. Deswegen, und vermutlich, weil G Data in Bochum angesiedelt ist und vom BSI als besonders qualifizierter Dienstleister gehandelt wird, hat die Behörde den Namen wohl als „Gefallen“ aus der Warnung herausgehalten, schlussfolgert der Spiegel. (wid@ct.de)

BSI-Warnung und Recherche: ct.de/yu6a

Verdächtige Mailanhänge risikolos untersuchen und entschärfen

Erfolgreicher Exorzismus

Wie Sie verdächtige Mailanhänge risikolos untersuchen und entschärfen

Mailanhänge zu öffnen, ist ein riskantes Unterfangen – aber oft unumgänglich. Wir stellen Tools vor, mit denen Sie Anhänge in risikofreie Kopien verwandeln und eingehend untersuchen

können, bevor Sie sie öffnen.

Von Sylvester Tremmel

Mailanhängen dürfen Sie nicht vertrauen. Doch egal wie vorsichtig Sie Ihren Posteingang auf Phishing-Attacken untersuchen und wie misstrauisch Sie E-Mails begegnen: Früher oder später taucht ein Anhang auf, dessen Absichten unklar sind und den Sie nicht ignorieren können, weil der Inhalt verspricht, wichtig zu sein.

Also müssen Sie irgendwie das Risiko verringern, das von dem Anhang ausgeht, bevor Sie ihn öffnen. Dazu haben Sie eine Reihe von Handlungsoptionen; die einfachste vorweg: Sehen sie nach, ob ein Online-Virenscanner wie virustotal.com den Anhang kennt. Allerdings nicht, indem Sie dort einfach die Datei hochladen, sonst haben Sie allzu leicht ein Datenschutzproblem am Hals (siehe dazu den Artikel auf S. 18). Berechnen Sie stattdessen lokal einen eindeutigen Hash der Datei und geben Sie diesen in die Suche von VirusTotal ein. Aus dem Hash lassen sich keine Daten rekonstruieren, aber falls es sich um eine bereits bekannte Datei handelt, bekommen Sie so eine Einschätzung des Dienstes. Viren-Dokumente werden in der Regel breit gestreut, mit etwas Glück liegt daher zu einer verseuchten Datei bereits ein Report vor.

Auf VirusTotal muss man nicht unbedingt eigene Dateien hochladen. Man kann auch per Hash nach bereits bekannten Dateien suchen.
Einen passenden Hash berechnen Sie am schnellsten auf der Kommandozeile, unter Windows mit dem PowerShell-Befehl Get-FileHash DATEI, unter Linux per sha256sum DATEI und unter macOS mit shasum -a 256 DATEI. Es gibt aber auch diverse Tools mit grafischer Oberfläche, die Hashes berechnen können; VirusTotal findet Hashwerte der Verfahren MD5, SHA-1 und SHA-256. (Nutzen Sie am besten das letzte, es gilt als uneingeschränkt sicher.)

Wenn gleich mehrere namhafte Scanner bei VirusTotal anschlagen, sollten Sie den Anhang direkt in den Orkus schicken. Falls der Onlinedienst die Datei nicht kennt oder darin nichts findet, dann ist das nur ein erster Hinweis, aber noch keine Unbedenklichkeitserklärung, und Sie sollten weiterforschen.

Ab in die Quarantäne

Zum Beispiel, indem Sie eine von Ihrem Arbeitsrechner isolierte Umgebung nutzen, aus der Malware nicht ausbrechen kann. Dafür eignet sich unter anderem eine virtuelle Maschine (VM). Wenn man darin ein bösartiges Dokument öffnet, geht

höchstens diese VM zugrunde. Zwar gibt es auch in VM-Software Lücken, aber das Risiko, dass eine Malware aus der Virtualisierung herauskommt, ist sehr, sehr gering.

VMs sind gut, um gelegentlich eine Datei zu analysieren. Dann bootet man darin am besten ein frisches Spezialsystem wie Kali Linux oder Parrot Security [1, 2] und löscht nach der Analyse die ganze VM. Sie können virtuelle Maschinen auch zur Absicherung der täglichen Arbeit nutzen, zum Beispiel, indem Sie darin ein wartungsarmes Linux wie Debian [3] installieren und damit Ihre Mails abrufen. Das ist eine gute Methode, aber wenn man täglich so arbeitet, stößt man schnell an die Grenzen, die durch die Isolierung entstehen. Wer dann keine eiserne Disziplin zeigt, bohrt über kurz oder lang Löcher in die Isolation, um leichter Dateien in die VM hinein und aus ihr heraus zu bekommen. Schlimmstenfalls wird aus der Isolations-VM allmählich die normale Arbeitsumgebung und der Schutzeffekt ist perdu.

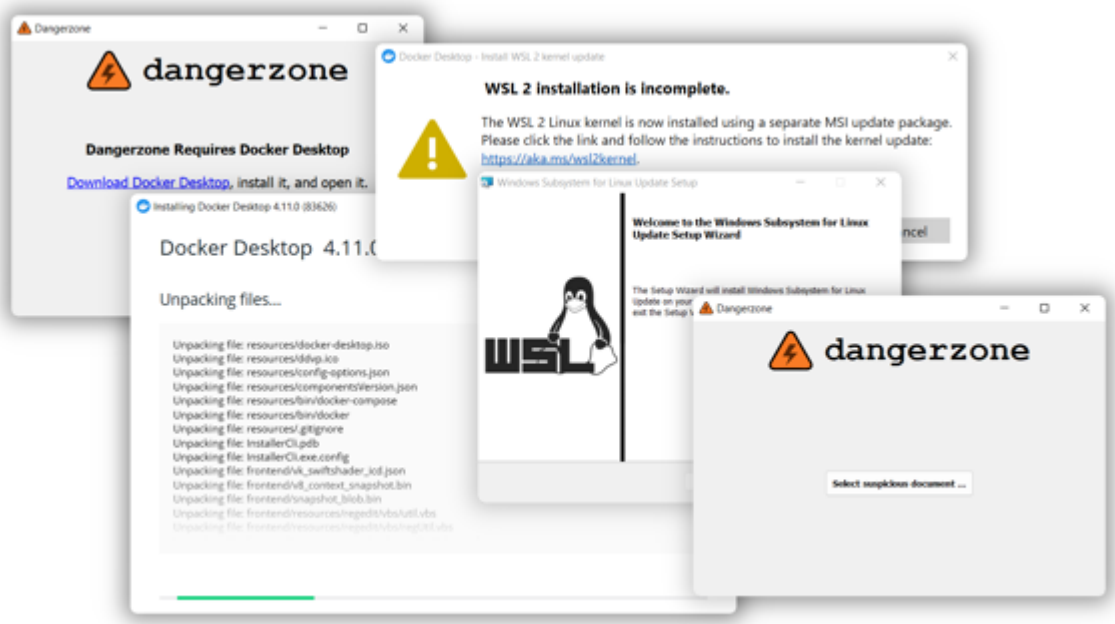
Praktikabler sind Tools, die automatische Isolationsumgebungen nutzen, um Dateien zu entschärfen, wie das Werkzeug Dangerzone (https://dangerzone.rocks). Es steht für Windows, macOS und Linux zur Verfügung und nutzt Container zur Isolation. Unter Windows und macOS kommt dafür Docker Desktop zum Einsatz unter Linux podman. Container bieten eine weniger gute Isolation als echte virtuelle Maschinen, stellen für Malware aber dennoch eine massive Hürde dar.

Die isolierten Container nutzt Dangerzone, um einen Anhang zu öffnen und in Bilddaten zu konvertieren. Malware können diese Pixelbilder nicht enthalten und nur diese Daten lässt Dangerzone aus dem Container. In einem zweiten Schritt wird aus den Pixeldaten ein PDF erzeugt, damit man keine lose Bildsammlung als Ergebnis erhält. Das Resultat ist ein PDF mit optisch gleichem Inhalt wie das Eingangsdokument, aber garantiert ohne Malware, Makros, versteckte Inhalte, verheimlichte Linkziele und viele andere Arten von Bedrohung. Als Betriebssystem im Container nutzt Dangerzone Linux (auch

unter Windows und macOS). Da die meisten Schädlinge auf Windows abzielen, ist es unwahrscheinlich, dass etwaiger Schadcode überhaupt ausgeführt wird, selbst wenn die Programme im Container Sicherheitslücken aufweisen sollten. Und auch wenn Malware die Software im Container kompromittiert und mit Linux zurande kommt, dann müsste sie immer noch aus dem Container ausbrechen, um Schaden anzurichten.

Bei so vielen Hürden kann man es verschmerzen, dass sich die Software im Container leider nicht leicht aktualisieren lässt: Der Installer von Dangerzone bringt ein fertiges Containerimage mit, damit die Software auch auf Rechnern ohne Internetzugang funktioniert. Wer sich nicht zutraut, das Containerimage selbst neu zu bauen – und eventuelle Inkompatibilitäten zu beheben –, bekommt erst mit einer neuen Dangerzone-Version ein neues Image. Das ist ein akzeptabler Kompromiss, aber wem er nicht reicht: Nichts spricht dagegen, noch eine Barriere hinzuzufügen und Dangerzone innerhalb einer VM zu betreiben.

Die Installation von Dangerzone erfordert unter Windows und macOS diverse Schritte, aber die sind relativ simpel: Zuerst laden Sie den Installer herunter und führen ihn aus. Danach können Sie Dangerzone bereits starten, erhalten aber den Hinweis, dass die Applikation Docker Desktop erfordert, sofern es nicht bereits installiert ist. Also folgen Sie dem angezeigten Link, laden Docker Desktop herunter und führen auch diesen Installer aus, was unter macOS mit ein paar Sicherheitsabfragen einhergeht, die Sie bestätigen müssen. Danach starten Sie Docker und sind unter macOS nach ein paar Sekunden Startzeit einsatzbereit.



Die Installation von Dangerzone erfordert zwar eine Reihe von Schritten, ist aber nicht kompliziert.
Unter Windows beschwert sich Docker Desktop eventuell, falls das „Windows Subsystem for Linux 2“ (WSL 2) nicht bereitsteht. Aber auch in diesem Fall zeigt die Problemmeldung direkt den nötigen Link an. Sie müssen also nur eine weitere Runde aus Klick, Download und Installation drehen und nun ist Docker auch unter Windows zufrieden und zur Arbeit bereit. Nach einem Klick auf „Check again“ merkt das auch Dangerzone und macht sich daran, das Container-Image zu installieren. Das geht vollautomatisch vonstatten.

Die Installation unter Linux ist leichter oder schwerer, je nachdem, um welche Distribution es geht. Für einige Distributionen betreiben die Dangerzone-Entwickler eigene Repositories, was die Installation sehr einfach macht. Unter Debian genügen beispielsweise folgende Befehle:

```
curl -s https://packagecloud.io/install/repositories/firstlookmedia/code/script.deb.sh | sudo bash
sudo apt update
sudo apt install -y dangerzone
```

Ein Skript per curl herunterzuladen und direkt auszuführen, gilt allerdings zu Recht als höchst fragwürdige

Installationsmethode. Wer dem Braten nicht traut, kann die Repositories manuell einrichten, die Dokumentation von Dangerzone erklärt, wie das geht (siehe ct.de/yw2x).

Leider unterstützt Dangerzone im Moment nur bei Debian aktuelle Versionen (11 und 12), bei Ubuntu und Fedora funktionieren von Haus aus nur etwas ältere Ausgaben (20.10, 21.04 und 21.10 beziehungsweise 33, 34 und 35). Auch bei anderen Distributionen sollten Sie sich nicht zu früh freuen: Beispielsweise findet sich Dangerzone zwar im User Repository von Arch Linux, allerdings ist das Paket aktuell nicht funktionstüchtig.

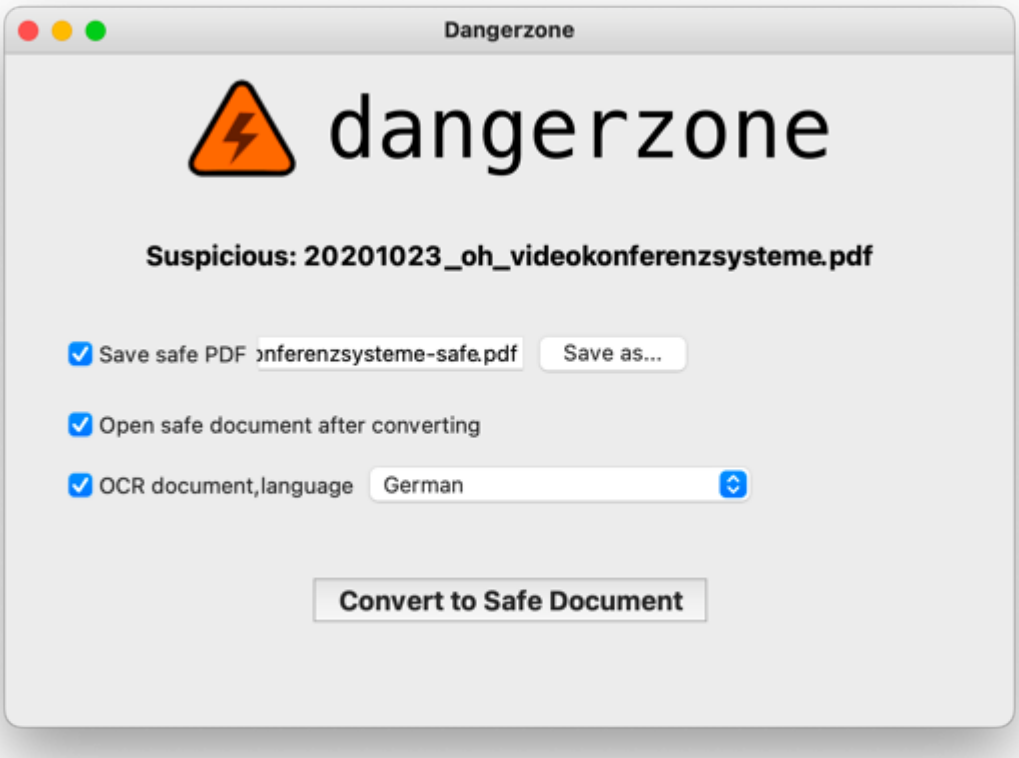
Statt sich unter Linux mit dem Paketbau oder Versionsinkompatibilitäten herumzuschlagen, bietet es sich an, einfach eine Debian-VM aufzusetzen und Dangerzone darin zu betreiben.

In der Gefahrenzone

Einmal fertig installiert, fällt die Bedienung von Dangerzone sehr leicht: Das Programm präsentiert nach dem Start nur eine Schaltfläche, die Sie drücken, um eine Datei zu konvertieren. Dangerzone kann diverse Office-Formate unschädlich machen, die ein Haupteinfallstor für Malware sind. Dazu startet das Programm im Container LibreOffice, um aus dem Office-Dokument ein PDF zu machen. Aus dem PDF werden dann Pixelgrafiken und daraus wieder ein – garantiert harmloses – PDF. Daneben können Sie mit Dangerzone auch PDFs und sogar Bilddateien entschärfen. Von letzteren geht nur eine geringe Gefahr aus, aber sicher ist sicher.

Nachdem Sie ein Dokument ausgewählt haben, bietet das Programm noch ein paar Einstellungen an. Dangerzone hat eine Texterkennung integriert (Optical Character Recognition, OCR) und fragt dafür nach der Sprache, in der das Dokument vermutlich verfasst ist. So kann das Tool im zweiten Schritt die Bilddaten analysieren, um den Textinhalt eines Dokumentes

zu rekonstruieren. OCR erhöht den Komfort erheblich, weil Sie dadurch im sicheren PDF Texte wieder markieren und kopieren können. Ein Klick auf „Convert to Safe Document“ stößt die Umwandlung an. Unter Linux und macOS erlaubt Dangerzone darüber hinaus, das Ergebnis-PDF automatisch zu öffnen, was Ihnen noch ein paar Klicks erspart.



Ein Klick und Dangerzone erzeugt eine garantiert harmlose Dateikopie mit dem gleichen (sichtbaren) Inhalt. So wird beispielsweise aus einem verseuchten Word-Dokument eine entschärfte PDF-Version.
Diese Bequemlichkeit können Sie unter Windows leicht nachrüsten, indem Sie die Kommandozeilenvariante von Dangerzone einspannen. Die wurde automatisch mitinstalliert, Sie können sie in der Eingabeaufforderung mit dem Befehl dangerzone-cli (für „command-line interface“) starten. Der Aufruf dangerzone-cli DATEI erstellt aus DATEI ein sicheres PDF, mit den Parametern --ocr-lang deu und --output-filename NEU.PDF schalten Sie die Texterkennung für Deutsch ein und legen den Namen der Ergebnisdatei fest.

Damit kann man leicht ein Skript basteln, das Dateien konvertiert und öffnet. Unter ct.de/yw2x haben wir Ihnen drei Varianten bereitgestellt: Eine Batch-Datei, ein AutoHotkey-Skript und eine daraus erstellte EXE-Datei. Es ist eine gute Idee, eines der Skripte als Standardanwendung für Office-Dateien festzulegen. In Zukunft genügt dann ein Doppelklick auf die Datei, um Dangerzone zu starten, eine sichere Version zu generieren und diese zu öffnen. So vermeiden Sie auch, gefährliche Dateien versehentlich direkt zu öffnen. Bei Bedarf können Sie die Originaldokumente über das Kontextmenü weiterhin mit der üblichen Anwendung öffnen – wenn Sie sicher wissen, dass sie harmlos sind.

Qubes OS

Wenn man willens ist, aus Sicherheitsgründen das Betriebssystem zu wechseln, stehen noch bessere Lösungen als Dangerzone zur Verfügung. Nahe am Nonplusultra liegt Qubes OS, das VMs nutzt, um das gesamte System in Sicherheitszonen zu unterteilen. Im Detail haben wir Qubes OS in Ausgabe 11/2022 vorgestellt [4].

Unter Qubes OS können Sie beliebige Dateien weitgehend gefahrlos öffnen, indem Sie im Kontextmenü „View in disposable“ oder „Edit in disposable“ auswählen. Das System startet dann automatisch eine aktuelle VM und öffnet darin den Anhang mit der Standardanwendung. Wenn Sie die schließen, verwirft Qubes OS die komplette VM. Einzig die Änderungen an der Datei werden zurückgeschrieben, sonst nichts, und auch die Änderungen nur, wenn Sie die „Edit“-Option gewählt haben.

Schon das liefert mehr Sicherheit und Komfort, als man mit normalen VM-Lösungen erreicht. Zusätzlich gibt es die Tools qvm-convert-pdf und qvm-convert-img. Diese Werkzeuge waren die Vorlage für Dangerzone und funktionieren im Prinzip genauso. Allerdings nutzen die Qubes-OS-Befehle echte VMs und keine Container. Das bietet noch mehr Schutz und ist leicht implementiert, wenn das Betriebssystem ohnehin alles in VMs

verpackt.

Mit spitzen Fingern

Trotz solcher Helferlein ist Dangerzone mit Einschränkungen verbunden. Zum einen stellt das LibreOffice im Container Office-Formate nicht unbedingt so dar, wie Microsoft Office unter Windows sie anzeigt; zum Beispiel, weil im Container Schriftarten fehlen. Sie müssen also damit leben, dass die Ausgabedokumente von Dangerzone eventuell ein bisschen anders aussehen, als die Eingabedateien.

Zum anderen holpert die Texterkennung von Dangerzone gelegentlich, besonders wenn die Schrift im Dokument schlecht lesbar ist, etwa weil es sich um eine schnörkelige Schreibschrift handelt. Längere kopierte Passagen sollten Sie daher Korrektur lesen.

Das Hauptproblem von Dangerzone folgt aber aus seiner Funktionsweise: Als Ergebnis erhalten Sie immer ein PDF. Das reicht, wenn Sie das Dokument nur betrachten wollen, aber wenn Sie ein Word-Dokument bearbeiten, eine Excel-Tabelle für Berechnungen nutzen oder ein PDF-Formular ausfüllen wollen, dann kommen Sie so nicht weiter.

Immerhin können – und sollten – Sie in solchen Fällen das Dokument erst einmal mit Dangerzone konvertieren und öffnen, um den Inhalt auf Plausibilität zu prüfen. Ein angeblicher Geschäftsbericht gehört direkt in die Tonne, wenn der sichtbare Inhalt laut Dangerzone nur aus einem aufwendigen Banner besteht, das Sie auffordert, Makros zu aktivieren.

Aber was, wenn der Dateiinhalt plausibel aussieht? In diesem Fall kommen Sie nicht darum herum, das Dokument zu öffnen – allerdings nicht mit der Standardanwendung! Als absolutes Minimum können Sie beispielsweise den PDF-Reader im Browser statt des Adobe Reader einspannen oder LibreOffice statt Microsoft Office. Das verringert zumindest die Chance, dass

eventuell im Dokument eingebetteter Schadcode korrekt ausgeführt wird (siehe S. 21).

Deutlich sicherer ist es aber, verdächtige Dateien mit Werkzeugen zu öffnen, die den Inhalt analysieren und nicht direkt anzeigen. Was für Werkzeuge sich dafür eignen, hängt vom Typ der fraglichen Datei ab. Wir beschränken uns im Folgenden auf die beiden verbreitetsten Arten von Anhängen: Office- und PDF-Dateien. Bilder werden zwar ebenfalls sehr häufig verschickt, aber von üblichen Formaten wie JPG oder PNG geht nur eine geringe Gefahr aus. Wer solche Dateien weiterverarbeiten will, kann sie – nach einer Inspektion per Dangerzone – in der Bildbearbeitung seiner Wahl öffnen. Das verbleibende Restrisiko ist sehr gering.

Zur Analyse von PDFs und Office-Dateien stellen wir Ihnen zwei Werkzeugsammlungen vor, die beide auf der Kommandozeile laufen. Lassen Sie sich davon nicht abschrecken, eine erste Analyse ist wirklich nicht schwer.

PDF-Tools

Der Sicherheitsforscher Didier Stevens hat eine Reihe von Werkzeugen geschrieben, um PDF-Dateien zu analysieren und bietet sie auf seiner Webseite als Zip-Archive zum Download an (siehe ct.de/yw2x). Um eine Datei grob einzuschätzen, eignet sich das Tool pdfid. Laden Sie das zugehörige Archiv von Didiers Website und entpacken Sie den Inhalt in ein beliebiges Verzeichnis. Das Tool ist in Python geschrieben; wie Sie die dafür nötige Laufzeitumgebung installieren, haben wir in c’t 5/2022 ausführlich erklärt [5].

Wenn Sie zum Beispiel die PDF-Datei verdaechtig.pdf mit

```
python pdfid.py verdaechtig.pdf
```

öffnen, gibt das Programm eine Liste von Schlüsselwörtern zurück, die es im PDF gefunden hat:

```
PDFiD 0.2.8 verdaechtig.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

Im Grunde sucht pdfid lediglich in der Datei nach diesen Schlüsselwörtern, die als ASCII-Zeichen vorliegen müssen. Wie so oft ist es in Praxis komplizierter: PDFs erlauben die Zeichenketten unterschiedlich zu kodieren, womit pdfid aber zurande kommt.

Achten sollten Sie besonders auf die Schlüsselwörter /JS und /JavaScript, die einen Wert größer 0 anzeigen, wenn das PDF vermutlich JavaScript-Code enthält. JavaScript kommt auch in einigen gutartigen PDFs vor, wo es beispielsweise Formulareingaben validiert. Nichtsdestotrotz sollten Sie JavaScript-Code als deutliches Warnsignal betrachten.

Ebenfalls Warnsignale stellen die Schlüsselwörter /AA, /OpenAction und /AcroForm dar. Werte größer 0 bedeuten dort,

dass der PDF-Reader automatische Aktionen starten soll, wenn man ein Dokument öffnet. Auch das kann harmlos sein und den Reader beispielsweise anweisen, eine bestimmte Seite des Dokuments anzusteuern – oder es führt Skriptcode aus und platziert Malware auf dem Rechner.

Wenn Sie auch nur eines dieser Schlüsselwörter entdecken, löschen Sie das verdächtige PDF, um auf Nummer sicher zu gehen. Wenn es dafür zu wichtig und dringend ist, dann hilft der Parameter --disarm (oder -d) von pdfid:

```
python pdfid.py -d verdaechtig.pdf
```

Das Programm produziert damit eine Kopie der Datei mit der Endung „.disarmed.pdf“. In der Kopie ist die Groß- und Kleinschreibung kritischer Schlüsselwörter vertauscht, aus /JavaScript wird /jAVAsCRIPT, aus /OpenAction wird /oPENaCTION und so weiter. So geschrieben handelt es nicht um gültige Schlüsselwörter und PDF-Reader sollten sie ignorieren. Diese entwaffnete Variante der Datei können Sie risikoarm öffnen.

Wem auch das nicht reicht, der kommt um eine detaillierte Analyse der internen Struktur des Dokuments nicht herum. Nur so findet man gefahrlos heraus, welche Aktionen genau ausgeführt würden und was genau der JavaScript-Code täte. Das erfordert allerdings Programmierkenntnisse, Wissen über den internen Aufbau von PDFs und mehr Platz, als dieser Artikel bietet. Wir werden in einer der folgenden Ausgaben zeigen, wie man bei so einer Analyse vorgeht.

Office-Dateien

Auch um Office-Dateien zu untersuchen, gibt es Kniffe und Werkzeuge in der Art von pdfid, aber nicht immer benötigen Sie dergleichen: Microsofts neuere Formate, die auf X enden (DOCX, XSLX, PPTX), sind im Grunde Zip-Archive, die lediglich einen speziellen Inhalt haben. Das hilft, falls Sie beispielsweise nur an den Bildern in einem Word-Dokument interessiert sind. Dann ändern Sie einfach die Endung von .docx in .zip, öffnen

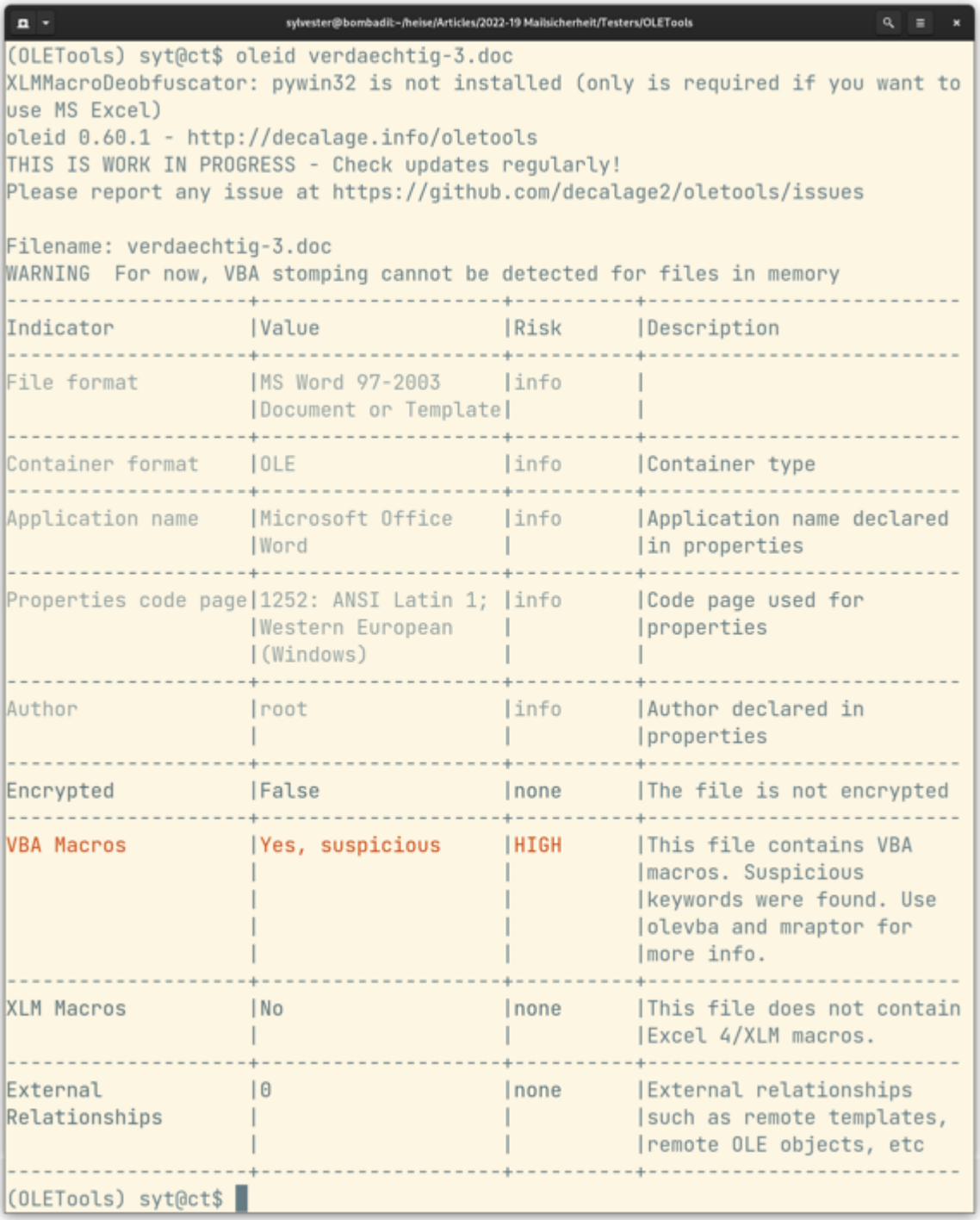
das Archiv mit dem Zip-Programm Ihrer Wahl und inspizieren die Bilder im entpackten Verzeichnis /word/media/.

Wenn Sie die Office-Dateien aber auf Unbedenklichkeit prüfen und letztlich in Word oder Excel bearbeiten wollen oder wenn es um ältere Formate geht (DOC, XLS …), dann funktioniert dieser Trick nicht. Was funktioniert, sind die oletools des Programmierers Philippe Lagadec (siehe ct.de/yw2x). Auch dieser Werkzeugkasten nutzt Python, am einfachsten installieren Sie ihn über die Paketverwaltung pip [5]:

```
pip install -U oletools[full]
```

Die oletools lesen sowohl die alten Office-Binärformate (wie DOC) als auch die aktuelleren auf XML-Basis (etwa DOCX). Für eine Einschätzung einer verdächtigen Datei ist das Programm oleid gedacht. Wie pdfid gibt es einen Überblick über relevante Aspekte einer Office-Datei. Statt einer bloßen Liste liefert oleid allerdings eine Tabelle samt Risikoeinschätzung der Elemente und schreibt im Fall der Fälle auch noch Handlungsanweisungen dazu (siehe Bild auf S. 31) Einer Word-Datei ohne Makros, externe Objekte oder andere Spezialitäten attestiert das Programm beispielsweise ein geringes Risiko: In der Spalte Risk sind alle Werte „info“ oder „none“.

Im Testdokument des heise Mailchecks (siehe S. 21) erkennt oleid korrekterweise ein VBA-Makro und bewertet es mit dem Risiko „Medium“. In der letzten Spalte steht, warum und was Sie jetzt tun können: „No suspicious keyword was found. Use olevba and mraptor for more info.“ Es wurden also keine Alarmsignale im Makro selbst gefunden, für Details soll man die Werkzeuge olevba oder mraptor nutzen.

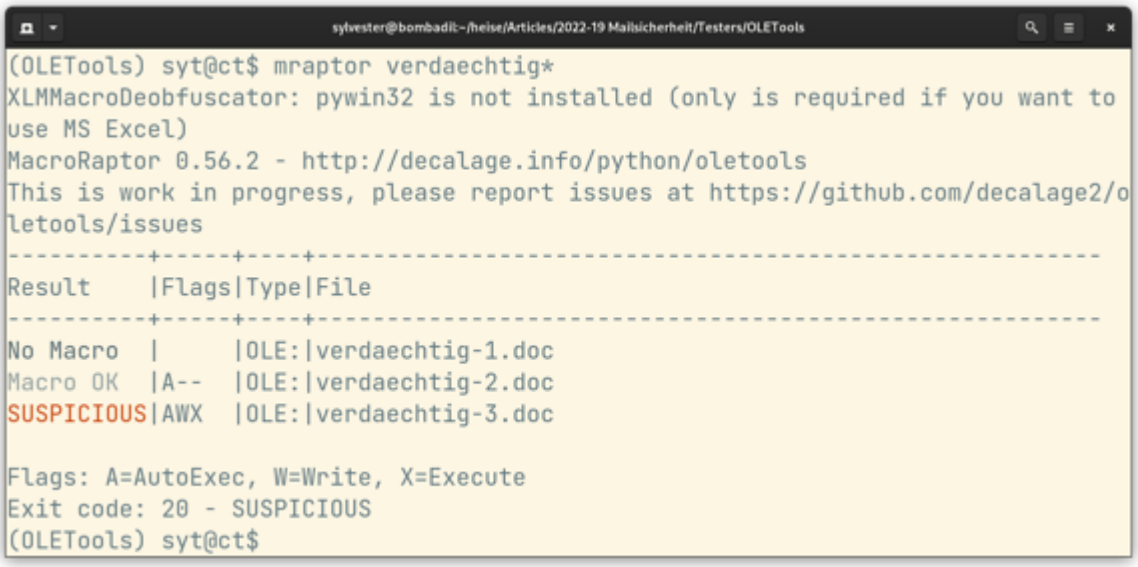


„VBA Macros: Yes, suspicious; Risk: HIGH“ meldet oleid und hat recht. Diese Datei ist tatsächlich höchst suspekt.
Ein Dokument mit einem höchst suspekten Makro, das versucht, eine Datei auf die Festplatte zu schreiben, bewertet oldid in Rot als „suspicious“ (verdächtig) und warnt in Großbuchstaben vor dem hohen Risiko, weil es verdächtige Schlüsselwörter im Makro gefunden hat.

Der wieder empfohlene Aufruf von mraptor erklärt den Verdacht näher: Das Makro wird automatisch ausgeführt („AutoExec“),

schreibt Daten („Write“) und versucht etwas außerhalb des Makro-Codes aufzurufen („Execute“). Folgerichtig kommt mraptor zu dem Schluss, dass die Datei verdächtig ist.

Wer es noch genauer wissen will, greift zum Werkzeug olevba. Es zeigt den enthaltenen Makrocode an, was aufschlussreich ist, wenn man Programmierkenntnisse hat. Zudem liefert olevba eine noch detailliertere Tabelle mit gefundenen problematischen Schlüsselwörtern und was sie bedeuten (siehe Listing auf S. 32).



mraptor kann man auch mehrere Dateien auf einmal vorwerfen. Er liefert dann eine Tabelle, ob Makros gefunden und als verdächtig bewertet wurden.

Listing: Output von olevba

```
+----------+--------------------+----------------------------
---------------+
|Type      |Keyword             |Description
|
+----------+--------------------+----------------------------
---------------+
|AutoExec  |AutoOpen            |Runs when the Word document
is opened      |
|Suspicious|Environ             |May read system environment
variables      |
|Suspicious|Open                |May open a file
```

```
|
|Suspicious|Write                  |May write to a file (if
combined with Open)  |
|Suspicious|Put                    |May write to a file (if
combined with Open)  |
|Suspicious|Binary                 |May read or write a binary
file (if combined |
|              |                                |with Open)
|
|Suspicious|CreateObject           |May create an OLE object
|
+----------+---------------------+-----------------------------
----------------+
```

Das Helferlein olevba extrahiert nicht nur Makrocode aus Office-Dateien (hier nicht gezeigt), sondern meldet auch, welche interessanten Begriffe sich im Code finden und worauf sie hindeuten.

Fazit

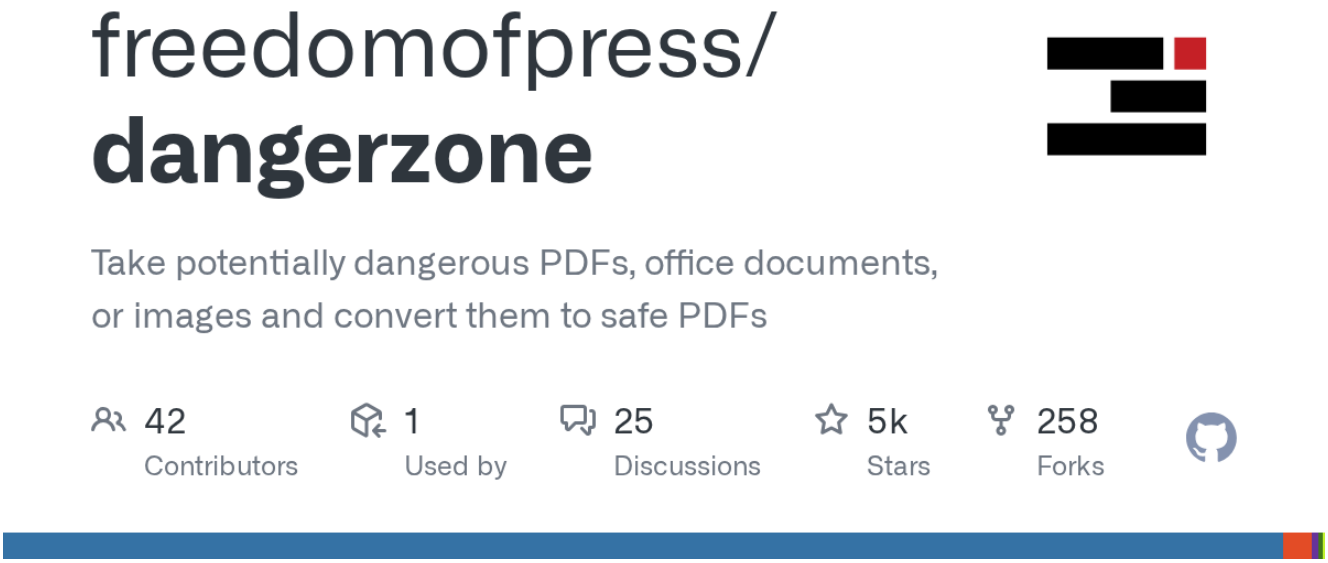
Auch ohne weitere Analyse müssen Sie keine Angst vor bösartigen Anhängen haben, wenn Sie die in diesem Artikel vorgestellten Werkzeuge einsetzen. Das Risiko, dass etwas den Filter von Dangerzone passiert, ist extrem gering. Übrigens sammeln sich unter Windows und macOS mit der Zeit immer mehr „Containers“ (mit Status „Exited“) und „Volumes“ in Docker Desktop an, zwei für jeden Aufruf von Dangerzone. Sie können die Einträge einfach ignorieren – oder aufräumen, wenn Sie die Unordnung stört. Löschen Sie einfach alle Exited-Container, die zugehörigen Volumes entsorgt Docker Desktop gleich mit. Dangerzone benötigt lediglich den Eintrag unter „Images“ und falls sie diesen versehentlich löschen sollten, legt das Programm ihn automatisch neu an.

Wenn Sie ein Dokument doch im Original öffnen müssen, dann reichen pdfid, oleid und Konsorten, um Gefahren zu wittern, bevor es zu spät ist. Das genügt für den Eigenschutz, aber wenn Sie die Neugierde packen sollte, dann sehen Sie sich

weiter in den Werkzeugkisten von Stevens und Lagadec um. Die enthalten noch viele weitere Programme, mit denen man den Inhalten von Office- und PDF-Dateien auf den Grund gehen kann. Ein Beispiel dafür werden wir in einer der kommenden Ausgaben beschreiben. (*syt@ct.de*)

1. Literatur
2. Ronald Eikenberg, Hacking-Stick, Kali Linux auf USB-Stick einrichten, c’t 23/2021, S. 30
3. David Wolski, Buntes Hacker-Linux, Linux-Distribution: Parrot Security für Pentester und Hacker, c’t 14/2020, S. 98
4. Sylvester Tremmel, Neue Stammkneipe, Wie Sie die passende Distribution für sich finden, c’t 3/2022, S. 30
5. Knut von Walter, Von Snowden empfohlen, Das sicherheitsorientierte Betriebssystem Qubes OS im Test, c’t 11/2022, S. 94
6. Ronald Eikenberg, Jan Mahn, Draufgebeamt, Python schnell und einfach einrichten, c’t 5/2022, S. 20

Downloads: ct.de/yw2x



Installing Dangerzone · freedomofpress/dangerzone Wiki

Take potentially dangerous PDFs, office documents, or images and convert them to safe PDFs — Installing Dangerzone · freedomofpress/dangerzone Wiki

PDF Tools

Here is a set of free YouTube videos showing how to use my tools: Malicious PDF Analysis Workshop. pdf-parser.py This tool will parse a PDF document to identify the fundamental elements used in the…

GitHub — decalage2/oletools: oletools — python tools to analyze MS OLE2 files (Structured Storage, Compound File Binary Format) and MS Office documents, for malware analysis, forensics and debugging.

oletools — python tools to analyze MS OLE2 files (Structured Storage, Compound File Binary Format) and MS Office documents,

for malware analysis, forensics and debugging. – GitHub – decalage2/oleto…

E-Mails richtig versenden

Verschickt und für gut befunden

Mails so verschicken, dass man Ihnen vertraut

Damit Ihre Mails nicht ungeöffnet als Spam oder Phishing aussortiert werden, sollten Sie es dem Empfänger so leicht wie möglich machen. Wenn Sie folgende Tipps beherzigen, verschicken Sie Mails, die einen guten Eindruck hinterlassen und auch tatsächlich gelesen werden.

Von Ronald Eikenberg

Absender, Betreff und Anrede

Der erste Eindruck zählt. Stellen Sie sicher, dass Sie einen aussagekräftigen Absendernamen in Ihrem Mailkonto eingestellt haben, etwa Vorname Nachname (Firma). Geben Sie Ihrer Mail einen sinnvollen, möglichst konkreten Betreff: anstatt „Anfrage“ beispielsweise „Kundenanfrage Ersatzteil XY für Modell Z“.

Beginnen Sie die Mail nach Möglichkeit mit einer individuellen Ansprache mit Person oder Firma, die Sie erreichen möchten. Stellen Sie eine Signatur mit Ihrem Namen, der Firma und Rufnummer für Rückfragen ein. So können die Adressaten Ihre

Mails zumindest von plumperen Fälschungen leicht unterscheiden.

Auf Empfänger achten

Überprüfen Sie vor dem Abschicken die Empfängerfelder „An“, „CC“ und „BCC“. Durch die automatische Vervollständigung Ihres Mailclients schleicht sich hier schon mal ein falscher Empfänger ein. Beim Beantworten von Mails sollten Sie in den Feldern gründlich ausmisten. Das gilt insbesondere für Antworten auf Mails, die an einen großen Empfängerkreis gerichtet waren. Denn die Antwort auf die Rundmail des Chefs muss in vielen Fällen nicht erneut die große Runde machen.

Wenn Sie mehrere Empfänger anmailen, die nichts miteinander zu tun haben, sollten Sie die Empfängeradresse unbedingt in das Feld BCC (Blindkopie) eintragen, damit die Empfänger nicht die gesamte Adressliste einsehen können. Wenn Sie „An“ oder „CC“ nutzen, geben Sie die Empfängerliste preis und handeln sich ein Datenschutzproblem ein.

Text statt HTML

HTML-Mails bergen unnötige Risiken: Der Empfänger sieht nicht auf den ersten Blick, auf welche Webadresse ein Link wirklich zeigt und von externen Servern eingebettete Inhalte sind entweder ein Datenschutzrisiko oder werden vom Empfängerclient nicht angezeigt. Verfassen Sie Ihre Mails daher besser im Textformat. Falls Sie auf eine URL verweisen möchten, sollten Sie Linkverkürzer wie TinyURL meiden, damit der Empfänger der Mail auf Anhieb weiß, wohin Sie ihn schicken möchten.

Vorsicht bei Anhängen

Von Mailanhängen geht eine große Gefahr aus. Phisher verschicken insbesondere Office-Dokumente und ausführbare Dateien, um neue Opfer in die Falle zu locken. Verschicken Sie Dokumente deshalb am besten im PDF-Format. Es hat sich als

risikoarmes Austauschformat durchgesetzt. Microsoft Office und viele andere Anwendungen können Ihre Dokumente im PDF-Format speichern, zum Beispiel über die Druckfunktion. Falls es doch mal ein Office-Format sein muss, dann wählen Sie bevorzugt die Formate, die auf X enden: DOCX, PPTX, XLSX. Diese können keine Makros enthalten.

Vermeiden Sie insbesondere ausführbare Dateiformate wie EXE. Dabei handelt es sich häufig um Malware, weshalb Mails mit ausführbaren Anhängen oft aussortiert werden. Kündigen Sie unerwartete und ungewöhnliche Mailanhänge am besten über einen anderen Kommunikationskanal an. Vermeiden Sie große Anhänge, da diese oft nicht ankommen.

Mails signieren

Im besten Fall signieren Sie ausgehende Mails digital vor dem Versand mit OpenPGP oder S/MIME. So hat der Empfänger die Chance, zu verifizieren, dass die Mail tatsächlich von Ihnen stammt. Mailverschlüsselung sollten Sie nur nutzen, wenn Sie sicher sind, dass der Empfänger die Mail tatsächlich entschlüsseln kann. Die Verbindung zum Mailserver sollte in jedem Fall transportverschlüsselt sein (möglichst SSL/TLS), was bei den meisten Mailanbietern inzwischen jedoch Standard ist.

Andere Kanäle nutzen

E-Mails sind ein denkbar schlechtes Transportmedium für wichtige Informationen: Sie werden meist unsigniert übertragen, deshalb kann der Empfänger Ihre Mail nur mit Mühe zweifelsfrei von Phishing unterscheiden. Nutzen Sie daher auch andere Kommunikationskanäle, die Ihnen zur Verfügung stehen. Diese sind häufig besser geeignet.

In Unternehmen gibt es für interne Kommunikation oft Chat- oder Kollaborationssoftware wie Teams, Slack oder Rocket.Chat, im Zweifel können Sie auch zum Telefonhörer

greifen. Messenger-Apps wie Signal oder WhatsApp sind ebenfalls besser als Mail, da die Nachrichten automatisch Ende-zu-Ende-verschlüsselt sind und der Empfänger den Absender überprüfen kann. Auch Dateien können Sie gut über diese Kanäle weitergeben.

Kurzlink zu diesem Artikel für Ihre Mail-Signatur: ct.de/sicher-mailen

(rei@ct.de)

26.08.2022 06:00 Uhr

c't Magazin

Von

- Ronald Eikenberg

Damit Ihre Mails nicht ungeöffnet als Spam oder Phishing aussortiert werden, sollten Sie es dem Empfänger so leicht wie möglich machen. Wenn Sie folgende Tipps beherzigen, verschicken Sie Mails, die einen guten Eindruck hinterlassen und auch tatsächlich gelesen werden.

Absender, Betreff und Anrede

Der erste Eindruck zählt. Stellen Sie sicher, dass Sie einen aussagekräftigen Absendernamen in Ihrem Mailkonto eingestellt haben, etwa Vorname Nachname (Firma). Geben Sie Ihrer Mail einen sinnvollen, möglichst konkreten Betreff: anstatt „Anfrage“ beispielsweise „Kundenanfrage Ersatzteil XY für Modell Z“.

Beginnen Sie die Mail nach Möglichkeit mit einer individuellen Ansprache mit Person oder Firma, die Sie erreichen möchten. Stellen Sie eine Signatur mit Ihrem Namen, der Firma und Rufnummer für Rückfragen ein. So können die Adressaten Ihre Mails zumindest von plumperen Fälschungen leicht

unterscheiden.

Auf Empfänger achten

Überprüfen Sie vor dem Abschicken die Empfängerfelder „An“, „CC“ und „BCC“. Durch die automatische Vervollständigung Ihres Mailclients schleicht sich hier schon mal ein falscher Empfänger ein. Beim Beantworten von Mails sollten Sie in den Feldern gründlich ausmisten. Das gilt insbesondere für Antworten auf Mails, die an einen großen Empfängerkreis gerichtet waren. Denn die Antwort auf die Rundmail des Chefs muss in vielen Fällen nicht erneut die große Runde machen.

Wenn Sie mehrere Empfänger anmailen, die nichts miteinander zu tun haben, sollten Sie die Empfängeradresse unbedingt in das Feld BCC (Blindkopie) eintragen, damit die Empfänger nicht die gesamte Adressliste einsehen können. Wenn Sie „An“ oder „CC“ nutzen, geben Sie die Empfängerliste preis und handeln sich ein Datenschutzproblem ein.

Text statt HTML

HTML-Mails bergen unnötige Risiken: Der Empfänger sieht nicht auf den ersten Blick, auf welche Webadresse ein Link wirklich zeigt und von externen Servern eingebettete Inhalte sind entweder ein Datenschutzrisiko oder werden vom Empfängerclient nicht angezeigt. Verfassen Sie Ihre Mails daher besser im Textformat. Falls Sie auf eine URL verweisen möchten, sollten Sie Linkverkürzer wie TinyURL meiden, damit der Empfänger der Mail auf Anhieb weiß, wohin Sie ihn schicken möchten.

Vorsicht bei Anhängen

Von Mailanhängen geht eine große Gefahr aus. Phisher verschicken insbesondere Office-Dokumente und ausführbare Dateien, um neue Opfer in die Falle zu locken. Verschicken Sie Dokumente deshalb am besten im PDF-Format. Es hat sich als risikoarmes Austauschformat durchgesetzt. Microsoft Office und viele andere Anwendungen können Ihre Dokumente im PDF-Format speichern, zum Beispiel über die Druckfunktion. Falls es doch mal ein Office-Format sein muss, dann wählen Sie bevorzugt die Formate, die auf X enden: DOCX, PPTX, XLSX. Diese können keine Makros enthalten.

Vermeiden Sie insbesondere ausführbare Dateiformate wie EXE. Dabei handelt es sich häufig um Malware, weshalb Mails mit ausführbaren Anhängen oft aussortiert werden. Kündigen Sie unerwartete und ungewöhnliche Mailanhänge am besten über einen anderen Kommunikationskanal an. Vermeiden Sie große Anhänge, da diese oft nicht ankommen.

Mails signieren

Im besten Fall signieren Sie ausgehende Mails digital vor dem Versand mit OpenPGP oder S/MIME. So hat der Empfänger die Chance, zu verifizieren, dass die Mail tatsächlich von Ihnen stammt. Mailverschlüsselung sollten Sie nur nutzen, wenn Sie sicher sind, dass der Empfänger die Mail tatsächlich entschlüsseln kann. Die Verbindung zum Mailserver sollte in jedem Fall transportverschlüsselt sein (möglichst SSL/TLS), was bei den meisten Mailanbietern inzwischen jedoch Standard ist. Lesen Sie auch

- Gefahrloser Umgang mit E-Mails

Andere Kanäle nutzen

E-Mails sind ein denkbar schlechtes Transportmedium für wichtige Informationen: Sie werden meist unsigniert

übertragen, deshalb kann der Empfänger Ihre Mail nur mit Mühe zweifelsfrei von Phishing unterscheiden. Nutzen Sie daher auch andere Kommunikationskanäle, die Ihnen zur Verfügung stehen. Diese sind häufig besser geeignet.

In Unternehmen gibt es für interne Kommunikation oft Chat- oder Kollaborationssoftware wie Teams, Slack oder Rocket.Chat, im Zweifel können Sie auch zum Telefonhörer greifen. Messenger-Apps wie Signal oder WhatsApp sind ebenfalls besser als Mail, da die Nachrichten automatisch Ende-zu-Ende-verschlüsselt sind und der Empfänger den Absender überprüfen kann. Auch Dateien können Sie gut über diese Kanäle weitergeben.

Geben Sie die Tipps weiter! Kurzlink zu diesem Artikel für Ihre Mail-Signatur: **https://ct.de/sicher-mailen**

Phishing-E-Mails erkennen und abwehren

E-Mails durchleuchtet

Phishing-Mails erkennen und abwehren

Der gefährlichste Ort im Internet ist Ihr Posteingang: Hinter jeder Mail kann ein Angriff stecken. Und die Zeiten, in denen man Phishing auf den ersten Blick erkennen konnte, sind längst vorbei. Mit den folgenden Tipps sortieren Sie auch die

kniffligen Fälle gekonnt aus.

Von Ronald Eikenberg

Die von Phishing-Mails ausgehende Gefahr wird gern unterschätzt, schließlich erkennt man die Fälschungen doch scheinbar schon aus zehn Meter Entfernung durch merkwürdige Absender wie „✩P.A.Y.P.A.L✩“, Betreffzeilen wie „Ihr Konto wurde begrenzt“ oder völlig schiefe Grammatik. Doch die Zeiten ändern sich: Solche tölpelhaften Mails gibt es zwar nach wie vor, sie bleiben jedoch meist im Spamfilter hängen und die wahre Gefahr lauert woanders.

Was es in den Posteingang schafft, ist von höherer Qualität. Perfekte 1:1-Kopien von echten PayPal- oder Rechnungsmails sind dabei noch das geringere Übel. Richtig gefährlich wird es, wenn die Absender mit echten Daten arbeiten, die sie zum Beispiel aus Datenleaks ziehen oder bei Personen aus Ihrem Umfeld erbeuten. Letzteres ist besonders gefährlich, denn es ist durchaus möglich, dass Sie heute eine Phishing-Mail von einer Person erhalten, mit der Sie gestern tatsächlich kommuniziert haben.

Dieses sogenannte Dynamit-Phishing nahm durch Emotet Fahrt auf und ist weltweit etlichen Firmen, Behörden, Bildungseinrichtungen und vielen mehr zum Verhängnis geworden. Die Schäden gehen in die Milliarden. Die Einstellung „Bei mir gibt es eh nichts zu holen“ ist übrigens fatal, denn Online-Schurken haben es nicht nur auf DAX-Konzerne abgesehen, sondern auf jeden. Ihr Instagram-Account oder Ihr Netflix-Zugang bringt den Phishern im Darknet zwar nur ein paar Dollar ein, doch wer große Stückzahlen verkauft, macht trotzdem einen guten Schnitt.

Mit den folgenden Strategien und Tipps sind Sie dazu in der Lage, verdächtige Mails zu erkennen und die richtigen Entscheidungen zu treffen, um nicht in die Phishing-Falle zu tappen. Es geht mit den offensichtlichen Warnsignalen los, die

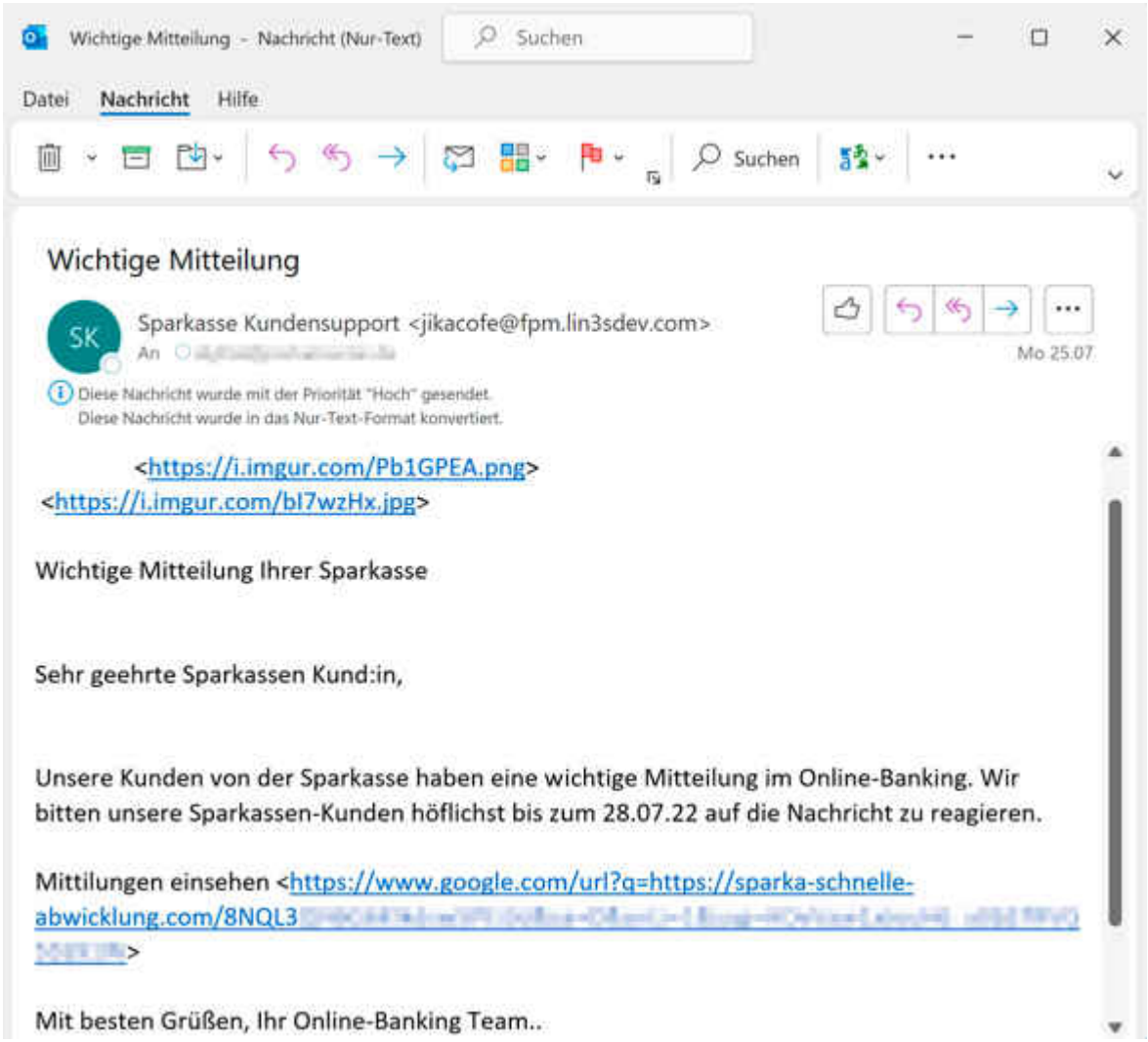
jeder kennen sollte, und weiter damit, wie Sie anhand der Mail-Innereien den Versandweg rekonstruieren und mithilfe des Sender Policy Framework (SPF) gefälschte Absender aufdecken.

Gut vorbereitet

Um keine unnötigen Risiken einzugehen, sollten alle verfügbaren Software-Updates für Betriebssystem, Browser und Mailprogramm installiert sein, da Updates häufig Sicherheitslücken schließen. Das gilt auch für alle Anwendungen, mit denen Sie Anhänge öffnen, allen voran Ihre Office-Suite und Ihr PDF-Viewer.

Stellen Sie Ihren Mailclient oder Webmail-Account am besten so ein, dass standardmäßig die Textversion einer Mail angezeigt wird, sofern möglich. Denn HTML-Mails können Sie leicht in die Irre führen, etwa durch ein offiziell anmutendes Äußeres oder gefälschte Links, die auf eine andere als die angezeigte URL verweisen. Im Textmodus sehen Sie das tatsächliche Linkziel auf den ersten Blick.

Seriöse HTML-Mails enthalten in der Regel eine Textversion mit demselben Inhalt, Ihnen entgeht also nichts. Falls Sie Thunderbird benutzen, klicken Sie für den Textmodus im Menü auf „Ansicht/Nachrichteninhalt/Reiner Text“, bei Outlook ist der Weg länger: „Datei/Optionen/Trust Center/Einstellungen für das Trust Center…/E-Mail-Sicherheit/Als Nur-Text lesen/Standardnachrichten im Nur-Text-Format lesen“.



Phishing entzaubert: Im Nur-Text-Modus wird sofort klar, dass an der angeblichen Sparkassen-Mail von Seite 17 etwas faul ist. Die Grafiken liegen beim Gratis-Bilderhoster Imgur, der Link „Mitteilungen einsehen“ nutzt eine Google-Umleitung auf sparka-schnelle-abwicklung.com.

Führt kein Weg an der HTML-Version vorbei, sollte Ihr Mailclient so eingestellt sein, dass er keine Inhalte aus externen Quellen lädt. Beim Abruf solcher Inhalte nimmt Ihr System direkten Kontakt mit dem Zielserver auf, wodurch der Absender erfährt, dass Sie die Mail geöffnet haben und Ihre Mailadresse tatsächlich existiert – es lohnt sich also, Sie mit weiteren Mails zu belästigen. Thunderbird und Gmail laden standardmäßig keine externen Inhalte, bei Outlook gibt es wenige Ausnahmen (etwa für bekannte Absender), die Sie im Trust Center unter „Automatischer Download“ konfigurieren können.

Plausibilitätscheck

Jetzt ist es Zeit für den obligatorischen Plausibilitätscheck: Kennen Sie den Absender? Erwarten Sie eine Mail von ihm? Ist sein Anliegen plausibel? Besteht auch nur der geringste Zweifel, sollten Sie weiter recherchieren, ehe Sie sich weiter auf die Mail einlassen und gar einen Link oder Anhang öffnen.

Stammt die Mail angeblich von einer Person, mit der Sie bereits in Kontakt standen – etwa Kollegen, Geschäftspartnern, Freunden oder Familie? Der einfachste Weg, für Klarheit zu sorgen, ist beim Absender nachzufragen, ob er die Mail tatsächlich verschickt hat. Nutzen Sie dazu keine Kontaktdaten aus der Mail (auch wenn sie auf den ersten Blick korrekt erscheinen), sondern eine Mailadresse oder Telefonnummer, über die Sie bereits in der Vergangenheit Kontakt hatten oder die von der legitimen Website des Absenders stammt.

Das Gleiche gilt für Zahlungsaufforderungen, Versandbestätigungen über nicht bestellte Ware, Anwaltsschreiben, Hinweise von Zahlungsdienstleistern und Banken sowie Mails, die Sie auffordern, sich auf einer Website einzuloggen. Recherchieren Sie die Kontaktdaten des angegebenen Absenders aus einer unabhängigen Quelle wie Google und fragen Sie nach. Wenn Sie einen Account beim angeblichen Absender haben, dann loggen Sie sich dort ein (wohlgemerkt nicht über einen Link aus der Mail) und sehen sie nach, ob sich auch dort die Mitteilung findet.

Es gehört zum guten Ton, dass Sie in Mails mit Ihrem Namen angesprochen werden, Unternehmen geben oft auch Ihre Kundennummer oder ähnliches mit an. Dies allein ist kein Beweis dafür, dass eine Mail unbedenklich ist, allerdings sollten Sie skeptisch werden, wenn ein an Sie gerichtete Mail keine persönliche Anrede enthält.

Auch der angegebene Absender kann eine Mail zwar be-, aber nicht entlasten: Bei E-Mails sind Absenderadresse und

Absendername frei wählbar, wie bei einer Postkarte. Sie können darüber also nicht zweifelsfrei feststellen, ob eine Mail echt ist. Nur die gegenteilige Feststellung ist möglich: Stammt die Mail von einer ungewöhnlichen Absenderadresse, dann ist ziemlich sicher etwas faul.

Bei Mails von Firmen und Behörden sollte die Absenderdomain zum Webauftritt passen, bei PayPal-Mails etwa paypal.de oder paypal.com. Offizielle Post werden Sie niemals von einer Freemail-Adresse (etwa @gmail.com oder @outlook.com) erhalten. Achten Sie bei der Absenderdomain penibel auf die Schreibweise, denn paypal.com ist eine andere Domain als paypa1.com oder paypal-kunden-support.com.

Wenn Sie sich unsicher sind, können Sie Absenderadresse zum Beispiel mit dem Reputationsdienst „Simple Email Reputation“ überprüfen (siehe ct.de/y2qp). Der Dienst liefert anhand zahlreicher Quellen wie Darknet-Leaks und Social-Media-Profilen eine Einschätzung, ob die Mailadresse vertrauenswürdig ist.

Der Webdienst „Simple Email Reputation“ schätzt ein, ob eine

Absenderadresse vertrauenswürdig ist. Dafür zapft er zahlreiche Datenquellen an.

Social Engineering

Phishing ist eine Social-Engineering-Attacke – die Angreifer versuchen Sie trickreich in die Falle zu locken. Bei Phishing-Mails werden Sie meist direkt oder indirekt aufgefordert, einen Anhang zu öffnen oder einen Link anzuklicken, doch die Fantasie der Online-Schurken kennt keine Grenzen. Bei der Chef-Masche (auch CEO-Fraud genannt), gibt sich der Absender als Ihr Chef aus und fordert Sie beispielsweise auf, eine dringende Überweisung auszuführen. Lassen Sie sich nicht davon einschüchtern.

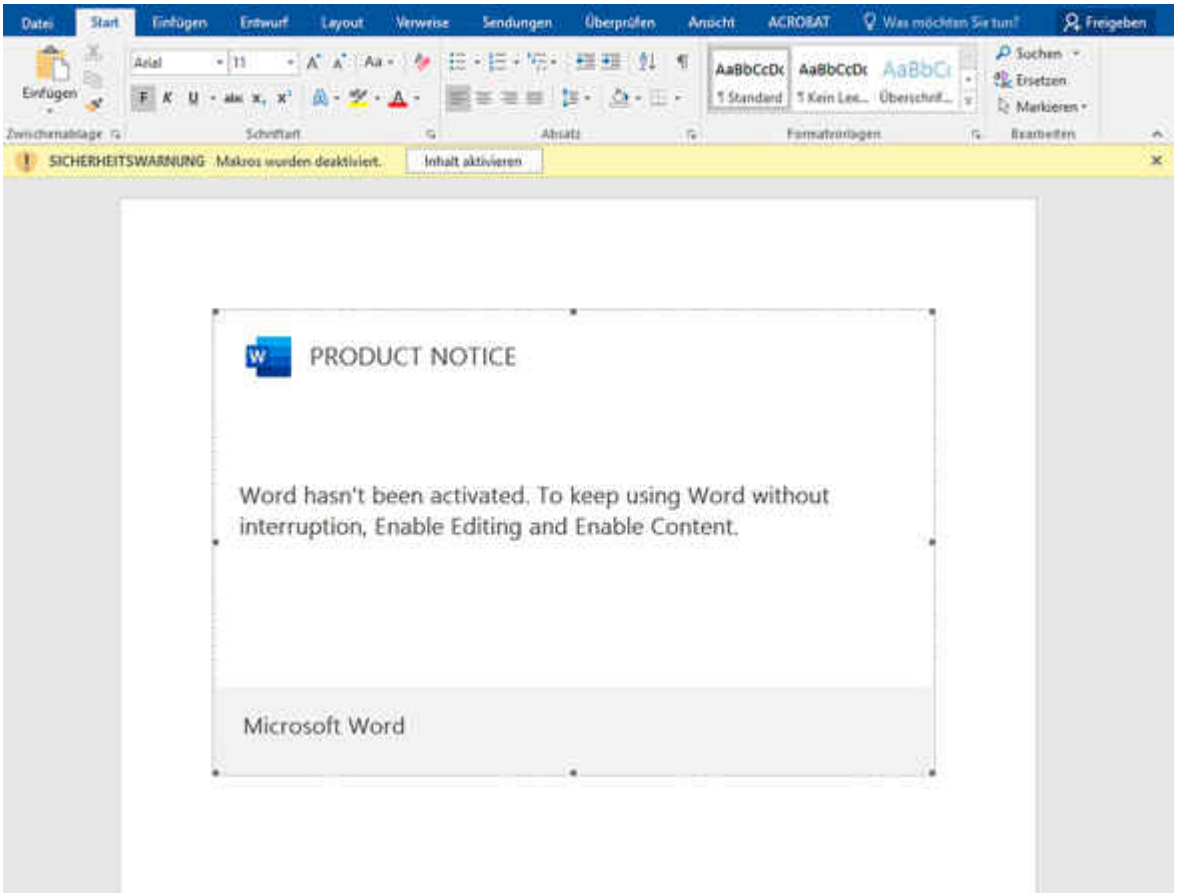
Gelegentlich verwickeln Sie die Betrüger auch in ein Gespräch, um zunächst eine Vertrauensbasis aufzubauen, ehe es ans Eingemachte geht. Geht es ums Geld, sollten den angegebenen Zahlungsempfänger genau überprüfen. Passen die angegebenen Bankdaten tatsächlich zu dem Unternehmen, das die Rechnung ausgestellt hat? Ist eine Bitcoin-Adresse oder eine ähnliche Krypto-Adresse im Spiel, handelt es sich mit hoher Wahrscheinlichkeit um einen Betrugsversuch.

Office ist Angreifers Liebling

E-Mail-Anhänge sind gefährlich – manche Dateiformate sind jedoch gefährlicher als andere. Angreifer haben es vor allem auf Microsoft Office abgesehen. Der Angriffscode steckt dann meist in Office-Makros, die den eigentlichen Schädling aus dem Internet nachladen und ausführen. Sie sollten bei Office-Dokumenten die gleiche Vorsicht walten lassen wie bei ausführbaren Dateien und sie erst mal nur mit der Kneifzange anfassen.

Sie erkennen Phishing-Dokumente zumeist daran, dass Sie nach dem Öffnen durch einen Text im Dokument aufgefordert werden, auf die gelbe Benachrichtigungsleiste oberhalb des Dokuments

zu klicken, um die Ausführung von Makros zu genehmigen. Achtung: Der Text und das Dokument selbst werden oft trickreich gestaltet, sodass der Inhalt nicht nach Word-Seite oder Excel-Tabelle aussieht, sondern wie ein offizieller Programmdialog. Konkret werden Sie gebeten, in der Leiste auf „Bearbeitung aktivieren“ und „Inhalt aktivieren“ zu klicken. Kommen Sie dieser Aufforderung auf keinen Fall nach.



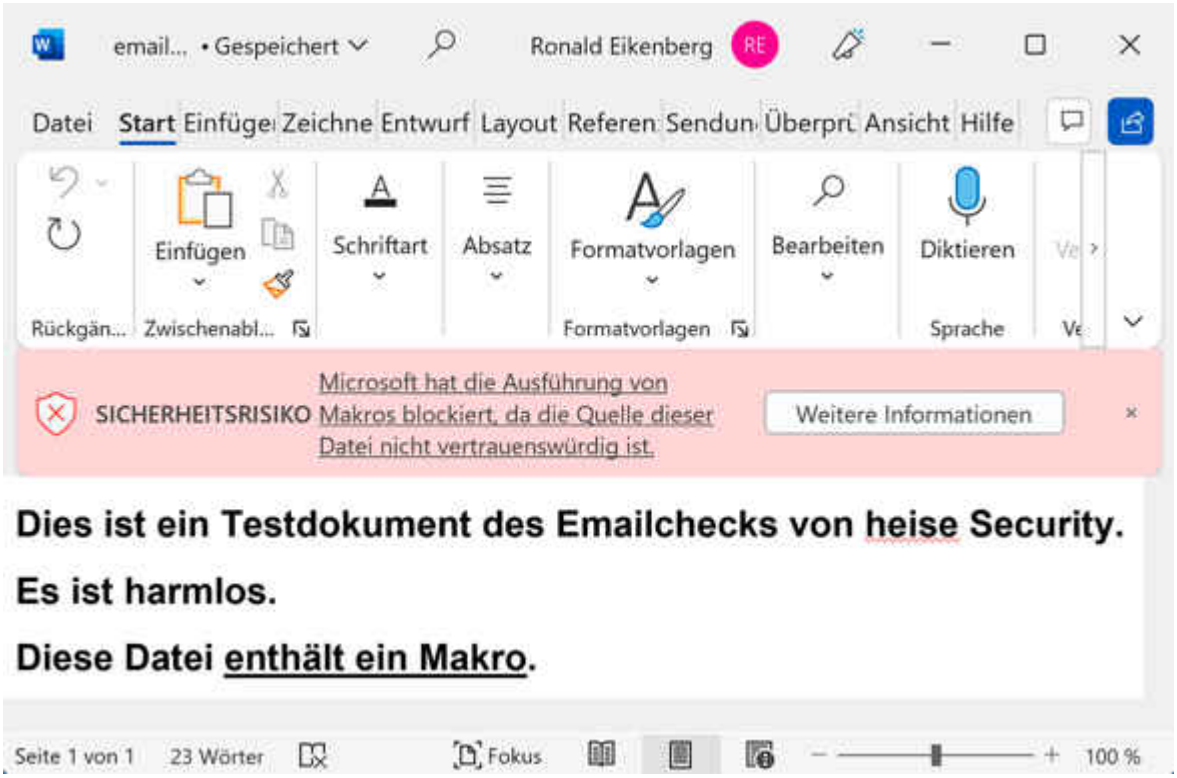
Phishing-Dokumente fordern häufig mit fadenscheinigen Argumenten dazu auf, auf die gelbe Leiste von Microsoft Office zu klicken. Dadurch wird das mitgelieferte Schadcode-Makro ausgeführt.
Kontrollieren Sie die Makro-Einstellungen in Ihrem Office, um sicherzustellen, dass Makros nicht automatisch ausgeführt werden. Klicken Sie hierzu auf „Datei/Optionen/Trust Center/Einstellungen für das Trust Center …“. Standardmäßig ist dort „Alle Makros mit Benachrichtigung deaktivieren“ eingestellt. Diese Einstellung begünstigt Phishing, weil man die Sperre über die gelbe Benachrichtigung umgehen kann.

Wenn Sie ohnehin nicht mit Makros arbeiten, schalten Sie diese

am besten mit „Alle Makros ohne Benachrichtigung deaktivieren“ aus. Falls Makros in Ihrer Firma eingesetzt werden, sollten diese digital signiert werden, damit Office die Echtheit überprüfen kann. Dann können Sie in Office „Alle Makros, außer digital signierte Makros deaktivieren“ einstellen.

Um zu überprüfen, wie Ihr Office auf Makros reagiert, können Sie sich über den Emailcheck von heise Security eine Testmail mit einer ungefährlichen Word-Datei zusenden lassen (siehe ct.de/y2qp). Wird der darin enthaltene Makro-Code ausgeführt, erscheint der Hinweis „Achtung! Makro wurde ausgeführt!“.

Aktuell ist Microsoft dabei, die Zügel weiter anzuziehen und Makros in Office-Dokumenten, die aus dem Internet stammen, standardmäßig zu blockieren. In solchen Fällen erscheint statt der gelben Leiste eine rote Warnung: „SICHERHEITSRISIKO: Microsoft hat die Ausführung von Makros blockiert, da die Quelle dieser Datei nicht vertrauenswürdig ist.“



Office blockiert neuerdings Makros in Dokumenten aus Online-Quellen mit rotem Alarm. Der Schutz ist allerdings lückenhaft. Ein echtes Hindernis ist dies jedoch nicht, man kann die Blockade leicht umgehen, indem man in den Dateieigenschaften

bei „Sicherheit:“ das Häkchen „Zulassen“ setzt. Es ist davon auszugehen, dass sich diese Handlungsanweisung in Kürze auch in den Phishing-Dokumenten wiederfinden wird. Zudem ist der Schutz keineswegs zuverlässig: Die Entscheidung, ob er aktiv wird, trifft Office anhand der Dateimarkierung Mark-of-the-Web (MOTW), die Dateien aus dem Internet kennzeichnet.

Das MOTW steckt in den Alternate Data Streams (ADS) einer Datei, die normalerweise unsichtbar sind. Wenn Sie einen Blick riskieren möchten, können Sie die ADS in der Windows-Eingabeaufforderung mit dir dokument.doc /R auflisten und das MOTW mit notepad dokument.doc:Zone.Identifier:$DATA anschauen. „ZoneId=3“ kennzeichnet Dateien aus dem Internet.

Die Markierung muss das Programm setzen, das die Datei heruntergeladen hat. Doch daran hält sich längst nicht jedes: Öffnet man ein Word-Dokument über Outlook, erscheint die oben zitierte Warnung. Öffnet man die gleiche Datei über Thunderbird, fehlt das MOTW und Word zeigt lediglich die übliche gelbe Leiste mit „Makros wurden deaktiviert“. Ein Klick auf „Inhalt aktivieren“ rechts daneben reicht aus, um den Code auszuführen.

Ist einer Mail ein Containerformat wie ZIP oder ISO angehängt, ist zwar der Container mit der MOTW markiert, häufig jedoch nicht die daraus geöffnete Office-Datei. Das wissen auch die Cyber-Banden: Laut der Security-Firma Proofpoint verschicken die Phisher verstärkt Container anstelle von bloßen Office-Dokumenten, um die Schutzvorkehrung zu umgehen.

Gute Formate, schlechte Formate

Die Liste der Dateiformate, die gefährlichen Schadcode ausführen können, ist sehr lang. Schon bei den Microsoft-Office-Formaten gibt es mindestens 17, die Makros mitschleppen können, darunter die alten Binärformate DOC, PPT und XLS. Microsoft Excel kann sogar das Textformat CSV zum Verhängnis werden.

Darüber hinaus gibt es unzählige weitere Dateiformate, die Schaden unter Windows anrichten können. Das weiß auch Microsoft, denn Outlook blockiert standardmäßig den Zugriff auf über einhundert Dateitypen von ADE bis XNK. Noch nie gehört? Wir auch nicht. Es gilt: Was man nicht kennt, öffnet man nicht.

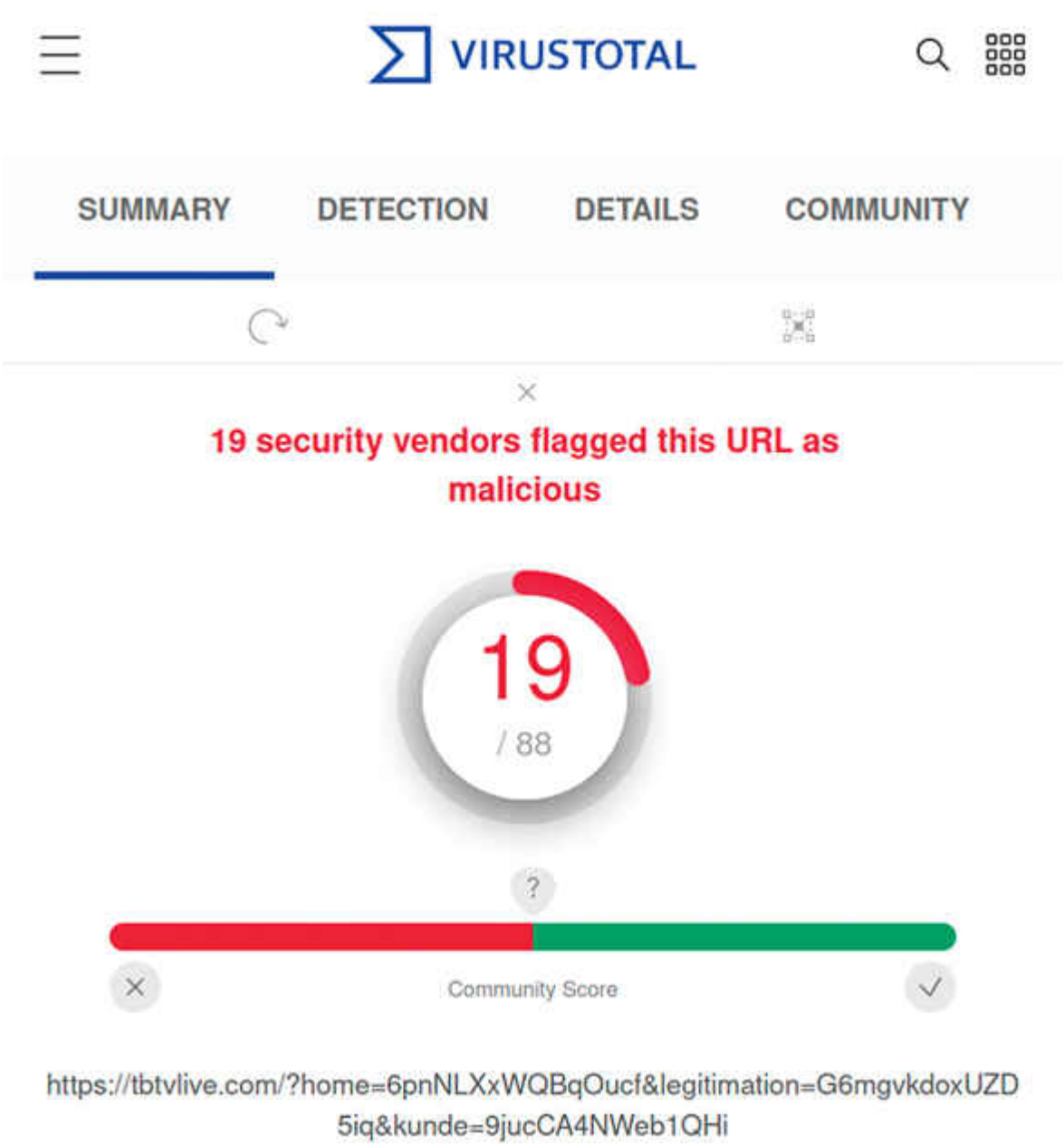
Höchst verdächtig sind verschlüsselte Dateien, wenn das dazugehörige Passwort in der Mail steht. Es handelt sich um einen alten Trick zur Verbreitung von Malware, denn Virenfilter können den Inhalt verschlüsselter Dateien nicht überprüfen. Selbst HTML-Dateien werden für Angriffe missbraucht, in solchen Fällen steckt die Phishing-Seite direkt im Anhang.

Wichtig zu wissen ist, dass die Office-Formate DOCX, PPTX und XLSX keine Makros enthalten können, von solchen Dokumenten geht also eine geringere Gefahr aus. Eine Unbedenklichkeitserklärung ist das jedoch nicht, denn selbst ohne Makros sind Angriffe möglich, zum Beispiel durch Sicherheitslücken in Office. Um das Risiko zu verringern, können Sie Office-Dokumente mit weniger verbreiteter Software wie LibreOffice öffnen. Die ist nicht per se sicherer, aber ein weniger wahrscheinliches Ziel für Angreifer.

PDF-Dateien sind ebenfalls nur mit Einschränkungen zu genießen, denn sie können JavaScript und eingebettete Dateien mit Schadcode enthalten. Öffnen Sie verdächtige PDFs besser nicht mit dem funktionsreichen Adobe Acrobat Reader, sondern mit dem Browser. Die PDF-Viewer der Browser unterstützen weniger PDF-Funktionen und bieten so eine geringere Angriffsfläche. Außerdem laufen sie eben im Browser und der ist darauf ausgelegt, mit nicht vertrauenswürdigen Inhalten aus dem Internet konfrontiert zu werden. Am besten untersuchen Sie die Office- und PDF-Dateien vor dem Öffnen, ob sie ausführbaren Code oder eingebettete Dateien enthalten. Wie das funktioniert, erfahren Sie ab Seite 28.

In seltenen Fällen, zum Beispiel im Rahmen staatlich initiierter Cyber-Angriffe, werden sogenannte Zero-Day-Lücken ausgenutzt, für die es noch keinen Patch gibt. Beispielsweise hat Microsoft im Mai eine hochgefährliche PDF-Datei entdeckt, die zunächst eine zum damaligen Zeitpunkt ungepatchte Lücke im Adobe Reader ausgenutzt haben soll, um anschließend über eine weitere Zero-Day-Lücke Windows zu attackieren. Die Datei soll zur Verbreitung der Spionagesoftware Subzero eines Wiener Herstellers gedient haben. Vor Zero-Day-Attacken können Sie sich kaum schützen, sie sind allerdings auch recht selten und richten sich eher gegen spezifische Ziele, nicht gegen die breite Masse der Anwender.

Insbesondere unter Windows sollte ein Virenschutz aktiv sein, der neue Dateien automatisch überprüft. Der vorinstallierte Windows Defender leistet gute Dienste. Ein Virenscanner erhöht die Chance, dass eine schädliche Datei frühzeitig auffliegt. Wird der Virenschutz nicht fündig, ist das jedoch keine Garantie dafür, dass eine Datei sauber ist. Sehen Sie davon ab, Dateianhänge, die persönliche oder vertrauliche Daten enthalten könnten, bei kostenlosen Online-Analysediensten wie VirusTotal oder Hybrid Analysis hochzuladen. Solche Dienste teilen die Dateien mit Dritten, etwa zu Forschungszwecken. Sie riskieren durch den Upload einen DSGVO-Verstoß.



Mailanhänge bei Online-Analysediensten wie VirusTotal hochzuladen ist keine gute Idee, da die Dienste die Dateien mit Dritten teilen. Verdächtige URLs können Sie den Diensten aber anvertrauen.

Lassen Sie sich nicht linken

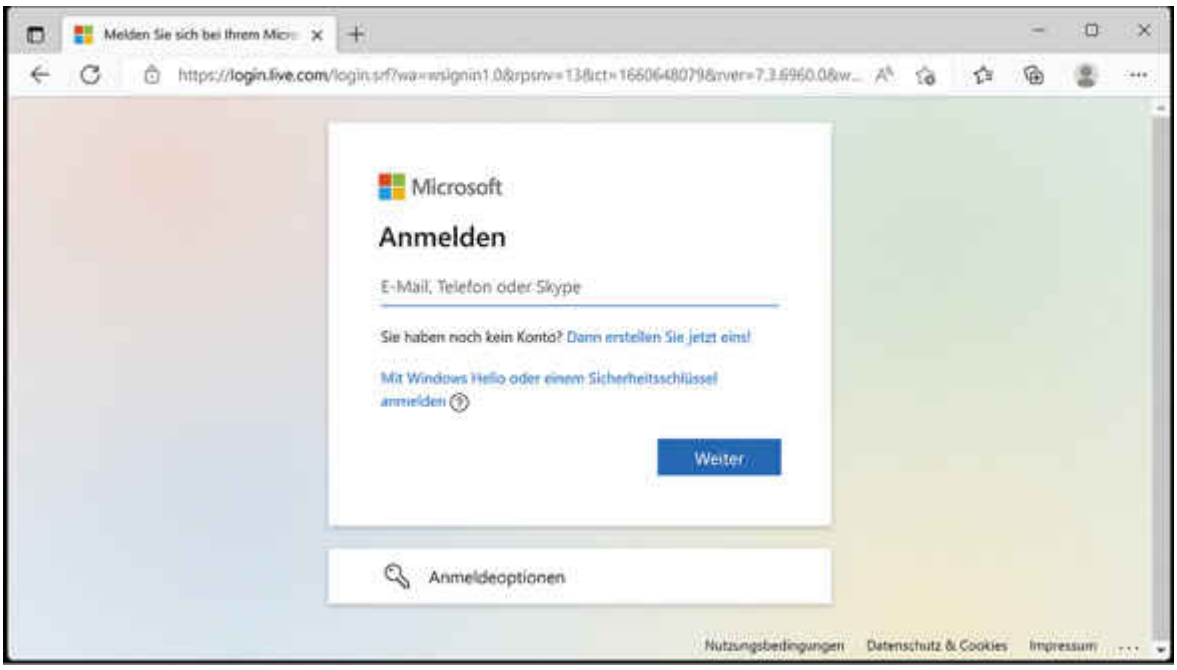
Nicht nur Dateianhänge können gefährlich sein, sondern auch Links. Stellen Sie wie oben beschrieben den Nur-Text-Modus im Mail-Client ein, damit man Ihnen keine manipulierten Links unterjubeln kann, deren Ziel von der angezeigten URL abweicht. Achten Sie außerdem darauf, dass die Zieladresse mit https:// beginnt. An diesem Präfix erkennen Sie Websites, die nach

Stand der Technik transportverschlüsselt (TLS/SSL) übertragen werden. Allerdings ist HTTPS kein Indikator dafür, dass sie der Website vertrauen können, da auch auch die meisten Phishing-Websites über HTTPS ausgeliefert werden.

Achten Sie penibel auf die Schreibweise der URL. Ein falscher Buchstabe, ein „I“ (großes „i“) anstelle eines „l“ (kleines „L“), reicht aus, um Sie auf eine völlig andere Website zu lotsen. Phisher verlängern legitime Domains auch gern durch unauffällige Zusätze, etwa „sparkasse-onlinebanking.de“ statt „sparkasse.de“. Steuern Sie im Zweifel immer die Ihnen bekannte, echte Adresse einer Website an, zum Beispiel über Ihre Booksmarks im Browser.

Falls Sie sich schon vor dem Besuch eines Links sicher sind, dass etwas faul ist, sollte Sie davon absehen, die verlinkte Website aus Neugier anzusteuern – nicht nur, weil dort etwa Malware auf Lücken in Ihrem Browser spitzen kann: Die Links sind häufig mit der Empfängeradresse verknüpft. Sie bestätigen Ihre Mailadresse durch das Aufrufen des Links. Meiden Sie auch demselben Grund auch Abmelden-Links (Unsubscribe) in Spam-Mails.

Zur Analyse verdächtiger Links können Sie verschiedene Online-Dienste nutzen: Browserling öffnet URLs in einer virtuellen Umgebung mit einem Browser Ihrer Wahl, VirusTotal befragt nach der Eingabe eines Links über 80 Security-Dienste und urlscan.io trägt diverse Informationen über eine Website zusammen, ehe ein Urteil darüber gefällt wird, ob sie Böses im Schilde führt (siehe ct.de/y2qp).



Die Single-Sign-on-Seite von Microsoft bauen Phisher besonders oft nach, weil sie die Türen vieler Unternehmen öffnet.

Zwei Faktoren, null Hacks

Zum Schutz vor Phishing zählt auch, auf den Ernstfall vorbereitet zu sein: Fällt man in der Hektik des Alltags doch mal auf eine gut gemachte Phishing-Mail rein, sollte der Schaden so gering wie nur irgendwie möglich sein. Aktivieren Sie bei allen wichtigen Diensten die Zwei-Faktor-Authentifizierung [1]. Dann ist zum Einloggen neben den Zugangsdaten ein weiterer Faktor nötig – beispielsweise ein Einmalpasswort in Form eines kurzzeitig gültigen Zahlencodes, den Sie mit einer Authenticator-App auf Ihrem Smartphone generieren.

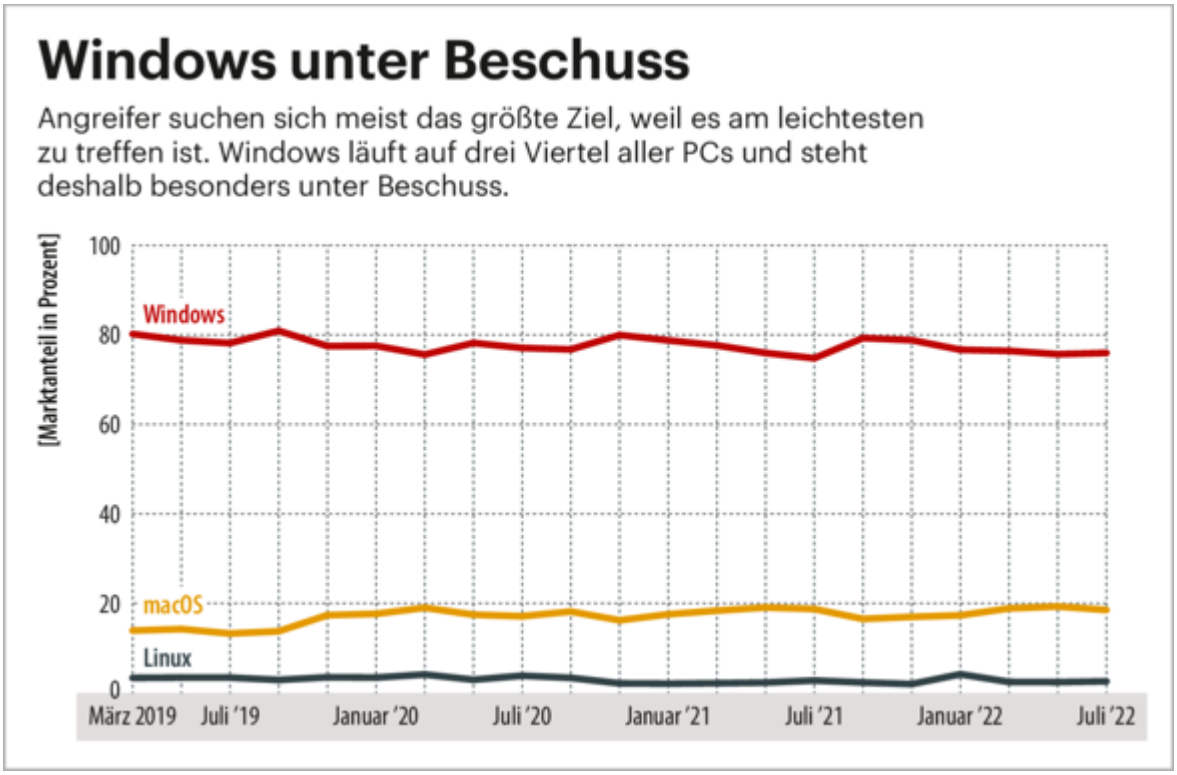
Haben Sie Ihre Zugangsdaten versehentlich einer Phishing-Website anvertraut, schauen die Cyber-Ganoven dann trotzdem in die Röhre, da sie sich ohne den zweiten Faktor nicht einloggen können. Gefährlich wird es allerdings, wenn Sie nicht nur Ihre Zugangsdaten, sondern auch das Einmalpasswort in die Phishingsite tippen. Für einen kurzen Moment ist dann ein Fremdzugriff möglich – Zeit genug, um automatisiert ein Session-Cookie vom Dienst abzurufen und Ihren Account damit dauerhaft zu übernehmen. Laut der Sicherheitsfirma Zscaler

richten sich solche Man-in-the-Middle-Angriffe auf den zweiten Faktor aktuell vor allem gegen Unternehmen, die Google- und Microsoft-Dienste einsetzen.

Davor schützt Sie der FIDO2-Standard, bei dem ein Sicherheitschip in Ihrem Rechner oder Smartphone den zweiten Faktor stellt. Alternativ können Sie auch einen USB-Sicherheitsschlüssel nutzen. Bei FIDO2 fließt automatisch die Domain der Website in die Berechnung des zweiten Faktors ein. Loggen Sie sich versehentlich auf der imaginären Phishing-Website paypa1.com mit FIDO2 ein, können die Online-Schurken die erbeuteten Daten deshalb nicht nutzen, um auf Ihr Konto bei paypal.com zuzugreifen.

Darüber hinaus gilt der alte, aber wichtige Tipp: Nutzen Sie möglichst für jeden Dienst ein anderes Passwort. So stellen Sie sicher, dass sich ein Angreifer mit erbeuteten Zugangsdaten nicht auch bei beliebig vielen weiteren Diensten einloggen kann. Die ganzen Passwörter müssen Sie sich weder merken noch ausdenken – ein Passwortmanager wie Bitwarden oder KeePass nimmt Ihnen die ganze Arbeit ab [2].

Auch das Thema Backups sollten Sie bei der Vorsorge für den Ernstfall nicht vernachlässigen. Cyber-Ganoven haben es auf Ihre Daten abgesehen und verschlüsseln diese, um von Ihnen anschließend ein Lösegeld zu erpressen. Damit sich in einem solchen Fall der Schaden in Grenzen hält, müssen Sie regelmäßig Backups Ihrer wichtigen Daten erstellen – insbesondere, wenn es um kritische Unternehmensdaten geht, ohne die der Geschäftsbetrieb nicht möglich ist.



Quelle: StatCounter

Risiko Windows

Wenn Sie mit Windows arbeiten, dann ist die von Phishing-Mails ausgehende Gefahr am größten: Angehängter Schadcode ist fast immer auf Windows abgestimmt. Das liegt nicht daran, dass Windows besonders unsicher ist, sondern vor allem an der enormen Verbreitung. Hierzulande läuft das Microsoft-Betriebssystem Statistiken zufolge auf rund 75 Prozent aller PCs, in Unternehmen dürfte der Anteil noch größer sein. Auf Platz 2 liegt macOS mit fast 20 Prozent.

Angreifer suchen sich meist das größte Ziel – also Windows, gefolgt von macOS. Je weniger verbreitet Ihr Betriebssystem ist, desto geringer ist die Wahrscheinlichkeit eines erfolgreichen Angriffs. Wenn Sie nicht auf Windows-Software angewiesen sind und ohnehin hauptsächlich im Browser arbeiten, lohnt es sich, einen Wechsel auf Linux oder Chrome OS in Betracht zu ziehen.

Bei den Mobilbetriebssystemen steht vor allem Android unter Beschuss, da man hier beliebige Apps als APK-Datei

installieren kann – ganz ohne den Store und die damit verbundenen Sicherheitsauflagen. Werden Sie unter fadenscheinigen Gründen aufgefordert, eine APK-Datei zu installieren, zum Beispiel ein vermeintliches Sicherheits-Update fürs Online-Banking, dann versucht ihnen jemand mit hoher Wahrscheinlichkeit einen Trojaner unterzujubeln. Bei iOS ist das Trojanerrisiko geringer, weil eine Infektion aufwendiger ist und etwa das Ausnutzen einer Sicherheitslücke erfordert.

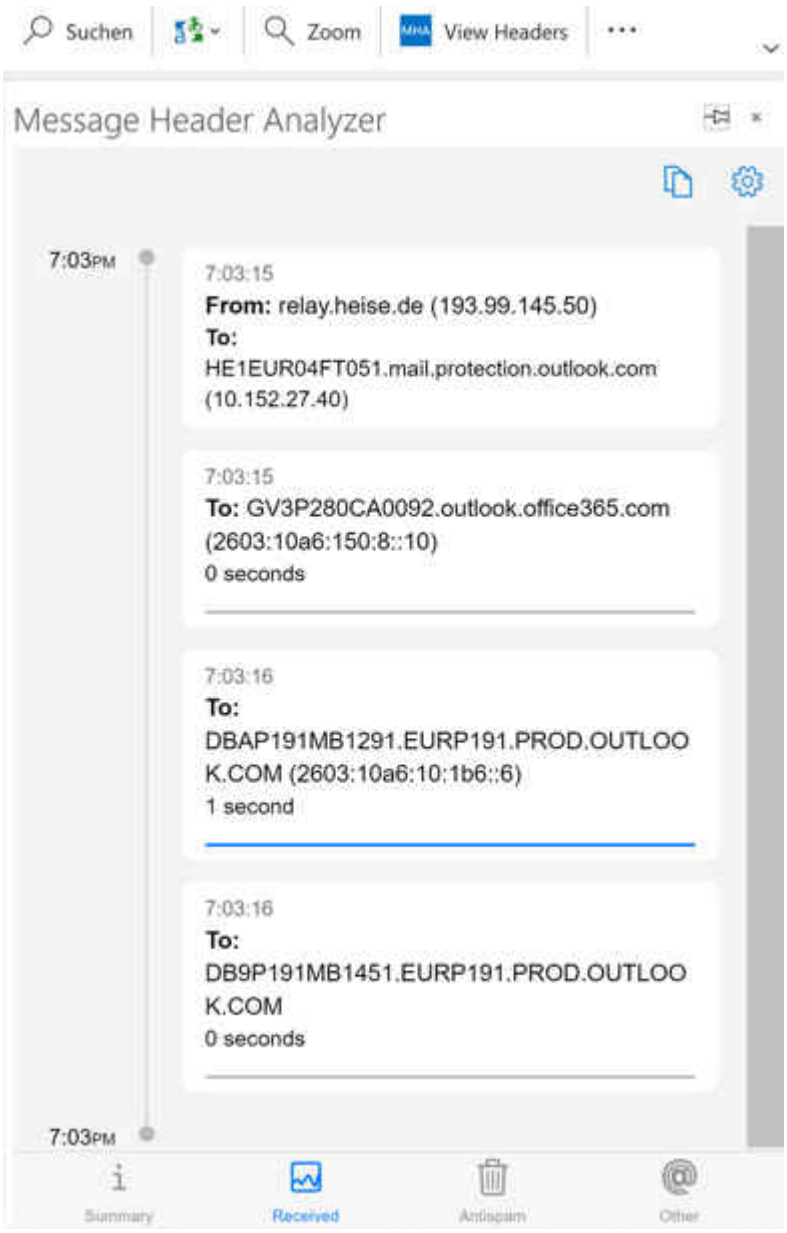
Achten Sie auch auf verdächtige Nachrichten aus sämtlichen Kanälen: Nicht nur Mails, auch WhatsApp-Nachrichten, SMS, Social Networks wie Facebook und Instagram, Anrufe und so weiter werden für Phishing missbraucht. Haben die Angreifer Kontaktdaten kopiert, kommt die Phishing-Nachricht womöglich sogar von einem Ihrer Freunde.

Herz und Nieren

Mit den oben beschrieben Maßnahmen sollten Sie die meisten Phishing-Fälle klären können, die größten Gefahren sind gebannt. Wenn Sie den Dingen gerne auf den Grund gehen, dann sollten Sie sich den Quelltext der verdächtigen Mail anzeigen lassen. Interessant ist vor allem der Header-Bereich oberhalb der eigentlichen Nachricht, denn hier gibt es viel zu entdecken; darunter der detaillierte Übertragungsbericht mit Informationen über das Mail-Relay, das die Mail eingeliefert hat.

Thunderbird-Nutzer finden den Quelltext einer gerade geöffneten Mail unter „Mehr/Quelltext anzeigen“. Wenn Sie Outlook nutzen, können Sie den Mail-Header wie folgt einsehen: Klicken Sie in der Nachrichtenliste doppelt auf eine Mail, um sie in einem eigenen Fenster zu öffnen, und anschließend auf „Datei/Eigenschaften“. Auch Webmailer bieten diese Funktion meist, bei Gmail klicken Sie nach dem Öffnen einer Mail unterhalb des Betreffs auf den Knopf mit den drei Punkten und „Original anzeigen“.

Welchen Weg die Mail genommen hat, verraten Ihnen die mit „Received:“ beginnenden Header-Zeilen von der untersten nach oben. Entscheidend ist der Übergabepunkt zum Eingangsserver Ihres Mail-Anbieters, bei einer Mail von rei@ct.de an eine Gmail-Adresse etwa: „Received: from relay.heise.de (relay.heise.de. [2a00:e68:14:800::19:19]) by mx.google.com […]“.



Der Mail Header Analyzer zeichnet den Versandweg einer Mail nach und zeigt nützliche Informationen aus dem Mail-Header an. Das Tool läuft im Browser und als Outlook-Add-In.

Um den Versandweg nachzuvollziehen, sind Analyse-Tools hilfreich, die automatisch die relevanten Zeilen im Mail-Code finden und in die richtige Reihenfolge stellen. Empfehlenswert

ist der „Message Header Analyzer“ des Microsoft-Mitarbeiters Stephen Griffin (siehe ct.de/y2qp), da das Tool Mails lokal im Browser auswertet. Outlook-Nutzer können es als Add-In ins Mailprogramm einklinken.

Die Mail wurde im obigen Beispiel vom Host relay.heise.de mit der IPv6-Adresse 2a00:e68:14:800::19:19 bei Google abgeliefert. Aber ist dieser Host tatsächlich für den angegebenen Absender rei@ct.de zuständig? Das können Sie im DNS-Eintrag der Absenderdomain nachschlagen. Die für die Domain zuständigen Mailserver sind dort in den sogenannten MX-Records vermerkt. Die MX-Records können Sie zum Beispiel über den Onlinedienst MXToolbox abfragen (siehe ct.de/y2qp).

Nach der Eingabe von ct.de listet der Dienst unter anderem auch relay.heise.de auf und ermittelt dazu die IP-Adresse, die der bereits bekannten aus dem Mail-Header entspricht – es passt also alles zusammen. Wenn Sie in der Zeile auf „Blacklist Check“ klicken, erfahren Sie auch gleich, ob der Mailserver auf Antispam-Blacklists steht.

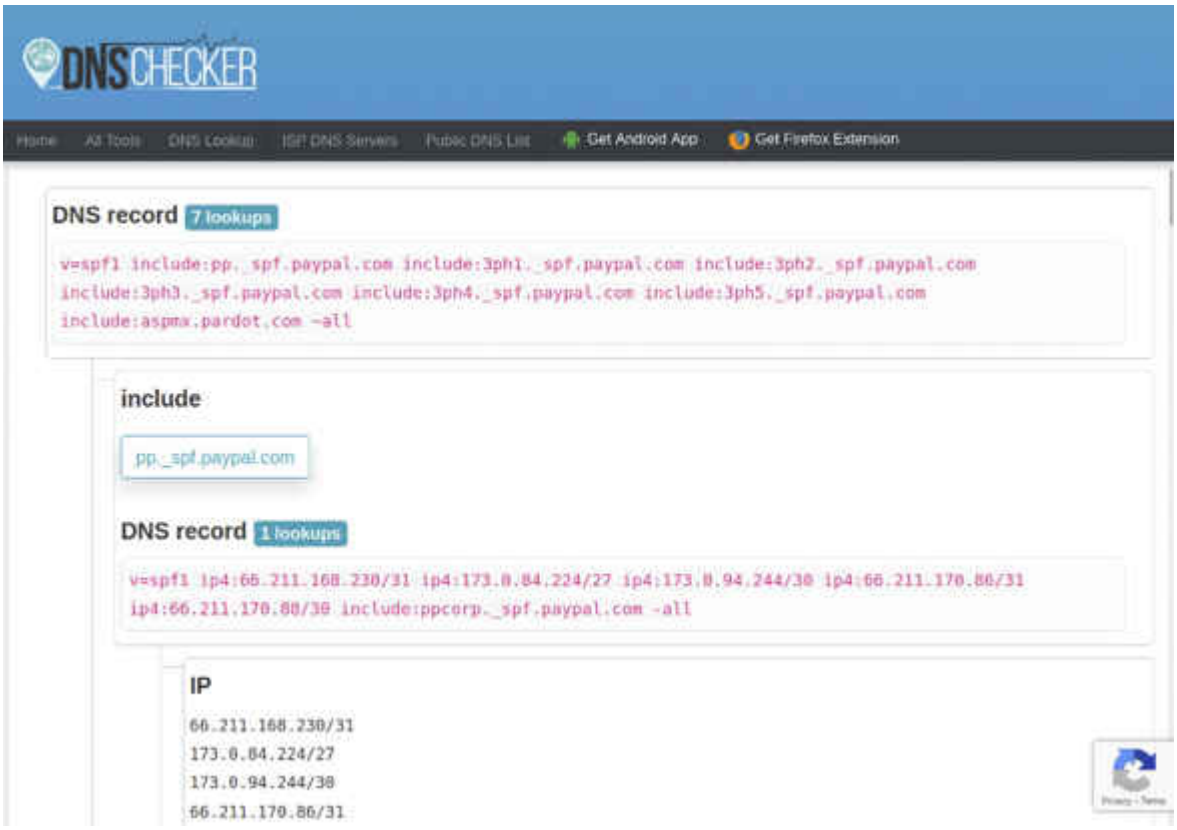
Anti-Spoofing-Check

Gespoofte Absender, also Absender mit gefälschter Mailadresse, stellen mittlerweile kein allzu großes Problem mehr dar. Das hat einen einfachen Grund: Solche Phishing-Mails kommen mit hoher Wahrscheinlichkeit nicht an. Das ist unter anderem dem Anti-Spoofing-Verfahren „Sender Policy Framework“ (SPF) zu verdanken. Damit können Admins im DNS-Eintrag ihrer Domains hinterlegen, von welchen IP-Adressen die Domains als Absender genutzt werden dürfen.

Der Empfangsserver kann beim Eintreffen einer Mail diese Informationen einfach per DNS-Abfrage abrufen und überprüfen, ob die IP-Adresse des einliefernden Mail-Relays auf der Whitelist steht. Im SPF-Eintrag kann vorgegeben sein, dass alle anderen IPs als „Fail“ zu behandeln sind, also als nicht autorisierte Absender. In diesem Fall wird ein moderner

Empfangsserver die Mail aussortieren, noch bevor sie den Posteingang erreicht.

Das Ergebnis der SPF-Überprüfung wird üblicherweise in den Header der Mail geschrieben, nachgelagerte Spamfilter und Mail-Clients können die Information also in die Risikobewertung einbeziehen. Mit dem oben erwähnten Add-on „Message Header Analyzer“ können Sie das Ergebnis auch in Outlook nachvollziehen, Gmail-Nutzer klicken im Menü der Nachricht auf „Original anzeigen“. Die SPF-Records eigener und fremder Domains können Sie zum Beispiel über den Webdienst „SPF Record Checker“ von DNS Checker (siehe ct.de/y2qp) herausfinden.



SPF macht es Phishern schwer, eine Domain als Absender zu missbrauchen. Mit dem SPF Record Checker überprüfen Sie, ob der Spoofing-Schutz für eigene und fremde Domains aktiv ist.
Wer selbst Mail-Accounts anbietet, ist gut damit beraten, nicht nur die SPF-Records eingehender Mails zu überprüfen, sondern auch für die eigenen Domains SPF-Einträge zu hinterlegen, damit die Domains nicht so leicht als Absender missbraucht werden können. Falls Sie externe Dienste mit der

Domain nutzen, etwa Newsletter-Dienstleister, müssen Sie auch diese in den SPF-Records hinterlegen.

Ein weiteres erwähnenswertes Schutzverfahren nennt sich „DomainKeys Identified Mail“ (DKIM). Damit lassen sich Mails digital signieren. Der Empfänger kann dann verifizieren, dass die Nachricht tatsächlich von einem Mailserver stammt, der für die Absenderdomain zuständig ist. Der Mailserver des Absenders nutzt zum Signieren einen geheimen Kryptoschlüssel, der dazu passende öffentliche Schlüssel muss im DNS-Eintrag der Domain hinterlegt sein.

Zum Anzeigen der DKIM-Daten aus dem Header können Outlook-Nutzer wieder das Add-on „Message Header Analyzer“ nutzen, Gmail-Nutzer klicken auf „Original anzeigen“. Für Thunderbird gibt es die Erweiterung „DKIM Verifier“ von Philippe Lieser (siehe ct.de/y2qp), die das Ergebnis der DKIM-Prüfung alltagstauglich im Kopfbereich jeder Mail anzeigt. Ausführliche Informationen über SPF, DKIM und DMARC, das beide Verfahren vereint, finden Sie in c’t 9/2019 [3].

PayPal-Phishing 2.0

Die Verfahren greifen allerdings nur, wenn die Phishing-Mail in irgendeiner Form technisch manipuliert und etwa mit einem gespooften Absender verschickt wurde. Nutzt der Absender ein eigenes oder kompromittiertes Mailkonto, schlagen SPF und DKIM nicht Alarm, weil die Mails über den legitimen Mailserver der Absenderadresse verschickt werden. Das Gleiche gilt, wenn es Online-Schurken gelingt, einen vertrauenswürdigen Dienstleister vor ihren Karren zu spannen.

Beispielsweise hat die Security-Firma Avanan beobachtet, dass Betrüger die PayPal-Funktion „Geld anfordern“ für Phishing missbrauchen. Darüber könnten PayPal-Nutzer Geldanforderungen an beliebige Mail-Adressen schicken. Der Empfänger bekommt auf diese Weise eine offizielle Mail von service@paypal.de mit gültiger DKIM-Signatur, die es mit hoher Wahrscheinlichkeit in

den Posteingang schafft. Der Absender kann einen bis zu 3500 Zeichen langen Text eingeben, der in der PayPal-Mail auftaucht. Vor solchen perfiden Phishing-Tricks können Sie sich nur selbst schützen: durch einen Plausibilitätscheck und eine gesunde Portion Skepsis.

Fazit

Die Tipps und Hintergründe in diesem Artikel helfen Ihnen dabei, Phishing-Mails zu erkennen, damit Sie nicht in die Falle tappen. Denn die wichtigste Verteidigung gegen solche Social-Engineering-Angriffe ist Wissen – insbesondere beim Bewerten von Dateianhängen und Links. Teilen Sie dieses Wissen mit anderen, damit auch Familie, Freunde und Kollegen nicht auf gefährliche Mails reinfallen. *(rei@ct.de)*

1. Literatur
2. Niklas Dierking und Ronald Eikenberg, Schlosskombination, Verfahren und Geräte für sichere Online-Zugänge, c't 9/2022, S. 18
3. Jan Schüßler und Marvin Strathmann, Ich kaufe ein ****, 25 Passwortmanager für PC und Smartphone, c't 5/2021, S. 16
4. Patrick Koetter, Wagenburg, Wie SPF, DKIM und DMARC gegen Phishing und Spoofing helfen, c't 9/2019, S. 174

Analysetools: ct.de/y2qp

Checkliste – E-Mail-Sicherheit

Checkliste: Mails so verschicken, dass man Ihnen vertraut

Damit Ihre Mails nicht aussortiert werden, sollten Sie es dem Empfänger so leicht wie möglich machen. Wenn Sie die folgenden Tipps beherzigen, gelingt das.

Lesezeit: 4 Min.

In Pocket speichern

vorlesen

Druckansicht Kommentare lesen 60 Beiträge

(Bild: Andreas Martini)
26.08.2022 06:00 Uhr

c’t Magazin

Von

- Ronald Eikenberg

Damit Ihre Mails nicht ungeöffnet als Spam oder Phishing aussortiert werden, sollten Sie es dem Empfänger so leicht wie möglich machen. Wenn Sie folgende Tipps beherzigen, verschicken Sie Mails, die einen guten Eindruck hinterlassen und auch tatsächlich gelesen werden.

Absender, Betreff und Anrede

Der erste Eindruck zählt. Stellen Sie sicher, dass Sie einen aussagekräftigen Absendernamen in Ihrem Mailkonto eingestellt haben, etwa Vorname Nachname (Firma). Geben Sie Ihrer Mail einen sinnvollen, möglichst konkreten Betreff: anstatt „Anfrage“ beispielsweise „Kundenanfrage Ersatzteil XY für Modell Z“.

Beginnen Sie die Mail nach Möglichkeit mit einer individuellen Ansprache mit Person oder Firma, die Sie erreichen möchten. Stellen Sie eine Signatur mit Ihrem Namen, der Firma und Rufnummer für Rückfragen ein. So können die Adressaten Ihre Mails zumindest von plumperen Fälschungen leicht unterscheiden.

Auf Empfänger achten

Überprüfen Sie vor dem Abschicken die Empfängerfelder „An“, „CC“ und „BCC“. Durch die automatische Vervollständigung Ihres Mailclients schleicht sich hier schon mal ein falscher Empfänger ein. Beim Beantworten von Mails sollten Sie in den Feldern gründlich ausmisten. Das gilt insbesondere für

Antworten auf Mails, die an einen großen Empfängerkreis gerichtet waren. Denn die Antwort auf die Rundmail des Chefs muss in vielen Fällen nicht erneut die große Runde machen.

Wenn Sie mehrere Empfänger anmailen, die nichts miteinander zu tun haben, sollten Sie die Empfängeradresse unbedingt in das Feld BCC (Blindkopie) eintragen, damit die Empfänger nicht die gesamte Adressliste einsehen können. Wenn Sie „An“ oder „CC“ nutzen, geben Sie die Empfängerliste preis und handeln sich ein Datenschutzproblem ein.

Text statt HTML

HTML-Mails bergen unnötige Risiken: Der Empfänger sieht nicht auf den ersten Blick, auf welche Webadresse ein Link wirklich zeigt und von externen Servern eingebettete Inhalte sind entweder ein Datenschutzrisiko oder werden vom Empfängerclient nicht angezeigt. Verfassen Sie Ihre Mails daher besser im Textformat. Falls Sie auf eine URL verweisen möchten, sollten Sie Linkverkürzer wie TinyURL meiden, damit der Empfänger der Mail auf Anhieb weiß, wohin Sie ihn schicken möchten.

Vorsicht bei Anhängen

Von Mailanhängen geht eine große Gefahr aus. Phisher verschicken insbesondere Office-Dokumente und ausführbare Dateien, um neue Opfer in die Falle zu locken. Verschicken Sie Dokumente deshalb am besten im PDF-Format. Es hat sich als risikoarmes Austauschformat durchgesetzt. Microsoft Office und viele andere Anwendungen können Ihre Dokumente im PDF-Format speichern, zum Beispiel über die Druckfunktion. Falls es doch mal ein Office-Format sein muss, dann wählen Sie bevorzugt die Formate, die auf X enden: DOCX, PPTX, XLSX. Diese können keine Makros enthalten.

Vermeiden Sie insbesondere ausführbare Dateiformate wie EXE. Dabei handelt es sich häufig um Malware, weshalb Mails mit ausführbaren Anhängen oft aussortiert werden. Kündigen Sie

unerwartete und ungewöhnliche Mailanhänge am besten über einen anderen Kommunikationskanal an. Vermeiden Sie große Anhänge, da diese oft nicht ankommen.

Mails signieren

Im besten Fall signieren Sie ausgehende Mails digital vor dem Versand mit OpenPGP oder S/MIME. So hat der Empfänger die Chance, zu verifizieren, dass die Mail tatsächlich von Ihnen stammt. Mailverschlüsselung sollten Sie nur nutzen, wenn Sie sicher sind, dass der Empfänger die Mail tatsächlich entschlüsseln kann. Die Verbindung zum Mailserver sollte in jedem Fall transportverschlüsselt sein (möglichst SSL/TLS), was bei den meisten Mailanbietern inzwischen jedoch Standard ist.

E-Mail-Sicherheit

Gute Mails, böse Mails

Gefahrloser Umgang mit E-Mails

Gefährliche Mails sollte man nicht öffnen – aber ob eine Mail harmlos ist oder nicht, weiß man oft erst, nachdem man sie geöffnet hat. Und manchmal nicht mal dann. Damit Sie trotzdem nicht in die Phishing-Falle tappen, müssen Sie ein paar Sicherheitsvorkehrungen treffen, die wir Ihnen hier geben.

Von Ronald Eikenberg

EMails zu öffnen ist wie Russisch Roulette – man weiß nie, ob es knallt. Meist hat man keine Wahl, ob man mitspielen möchte. Versuchen Sie doch mal, Ihrem Chef zu erklären, dass Sie ab sofort keine E-Mails mehr öffnen. Schlagkräftige Argument hätten Sie zuhauf: E-Mails sind gefährlich und der wichtigste Verbreitungsweg für Schädlinge. Allein die berüchtigte, hauptsächlich per Phishing-Mail verbreitete Emotet-Malware hat weltweit unzählige Unternehmen, Behörden, Krankenhäuser & Co. lahmgelegt und dabei Schäden in Milliardenhöhe angerichtet.

Ein weiteres Argument ist, dass Sie Ihrem Chef nicht versprechen können, dass Sie alle Phishing-Mails aussortieren und nicht darauf reinfallen. Denn die Zeiten, in denen man solche Mails schon von Weitem erkennen konnte, sind längst vorbei. Angreifer nutzen immer häufiger echte – gestohlene – Daten, um Sie in die Falle zu locken, zum Beispiel plausible Absender, mit denen Sie bereits Kontakt hatten. Phishing-Mails zitieren mitunter sogar aus vorangegangenen Mailwechseln mit Kollegen, Partnerfirmen oder Kunden.

Zwickmühle E-Mail

Wer beruflich mit Mails arbeitet, muss nicht selten Dutzende oder gar Hunderte davon Tag für Tag bearbeiten – und genauso viele Entscheidungen treffen. Das ist ganz schön viel Verantwortung, denn jede Fehlentscheidung, jeder falsche Klick kann die ganze Firma über Wochen lahmlegen. Die Krux ist, dass man es sich aber auch nicht leisten kann, eine Kundenanfrage oder eine Auftragsmail zu übersehen. Jede Mail muss daher gecheckt werden.

Sie ahnen es vielleicht bereits: Auch mit den besten Argumenten kommen Sie aus der Nummer nicht raus. E-Mail ist

der kleinste gemeinsame Nenner bei der Online-Kommunikation und daher weiterhin unverzichtbar. Die interne Kommunikation kann man inzwischen gut über moderne Kollaborationssoftware wie Rocket.Chat, Slack oder Teams abwickeln, für die Kommunikation mit der Außenwelt gibt es jedoch keinen Ersatz mit breiter Akzeptanz.

Im Privatleben sieht es ähnlich aus: Freunde und Verwandte können Sie problemlos über Messenger-Apps wie WhatsApp oder Signal erreichen – Ende-zu-Ende-verschlüsselt nach Stand der Technik und mit überprüfbarem Absender. Für die Kontaktaufnahme mit Firmen, Behörden und vielen mehr müssen Sie jedoch oft noch eine Mail schreiben. Rechnungen, Versandbestätigungen, Benachrichtigungen über verdächtige Aktivitäten et cetera landen in Ihrem Posteingang, neben Phishing-Mails aller Art. Und es bleibt an Ihnen hängen, die guten Mails von den bösen zu unterscheiden.

Aber was tun? Phishing zählt zur Angriffskategorie „Social Engineering“ – die Angreifer zielen also nicht auf technische Sicherheitslücken ab, sondern auf die Schwachstelle Mensch. Genau hier setzen die folgenden Artikel an: Wir möchten Ihnen das nötige Wissen und einige praktische Tipps an die Hand geben, damit Sie leicht die Spreu vom Weizen trennen können und für Phishing-Mails nur noch ein müdes Lächeln übrig haben.

Phishing auf den zweiten Blick: Mittlerweile muss man genau hinsehen, um die Rechtschreibfehler von Online-Ganoven zu finden. In der Anrede wird hier sogar ein bisschen gegendert.

Mails entschärfen

Es geht nicht nur darum, wie Sie verdächtige Mails anhand offensichtlicher und versteckter Merkmale bewerten können (siehe S. 18), sondern auch um die kniffligen Fälle. Manchmal bleiben auch nach einer eingehenden Prüfung Restzweifel, ob es

sich um Spreu oder Weizen handelt und ob die angehängte Datei unentbehrlich ist oder ernstzunehmenden Schaden anrichtet.

In solchen Fällen können Sie den Anhang vor dem Öffnen mit einem Tool wie Dangerzone entschärfen, indem Sie ein harmloses PDF daraus machen – garantiert ohne Office-Makros. Oder Sie analysieren die Datei mit speziellen Tools, um vorab gefahrlos zu überprüfen, ob sich darin Makros oder eingebettete Dateien verstecken (siehe S. 28).

Wir möchten Sie dazu anregen, dieses Wissen auch mit Kollegen, Freunden, Familie und Geschäftspartnern zu teilen – in ihrem eigenen Interesse. Denn den größten Einfluss auf Ihren Posteingang haben nicht Sie, sondern die Absender der Mails. Wenn jeder die wichtigsten Dos & Don’ts kennt und beim Verschicken beherzigt, wird E-Mail für alle sicherer.

Wir haben die wichtigsten Tipps für den Mailversand daher als kompakte und leicht verdauliche Checkliste auf Seite 26 zusammengestellt. Die Checkliste ist online frei abrufbar, damit Sie sie leicht weitergeben können. Wenn Sie mögen, können Sie in Ihrer Mailsignatur darauf verweisen: **https://ct.de/sicher-mailen** (*rei@ct.de*)

Datenleck in Österreich durch Azure-Workflow

Rausgerutscht

Datenleck in Österreich durch Azure-Workflow

Interne Links einer Microsoft-Azure-Anwendung sind in den Suchindex von Bing geraten – personenbezogene Daten waren dadurch öffentlich einsehbar. Eine Spurensuche offenbart, wie schnell vermeintlich geheime Links zum Sicherheitsrisiko werden – nicht nur bei Azure.

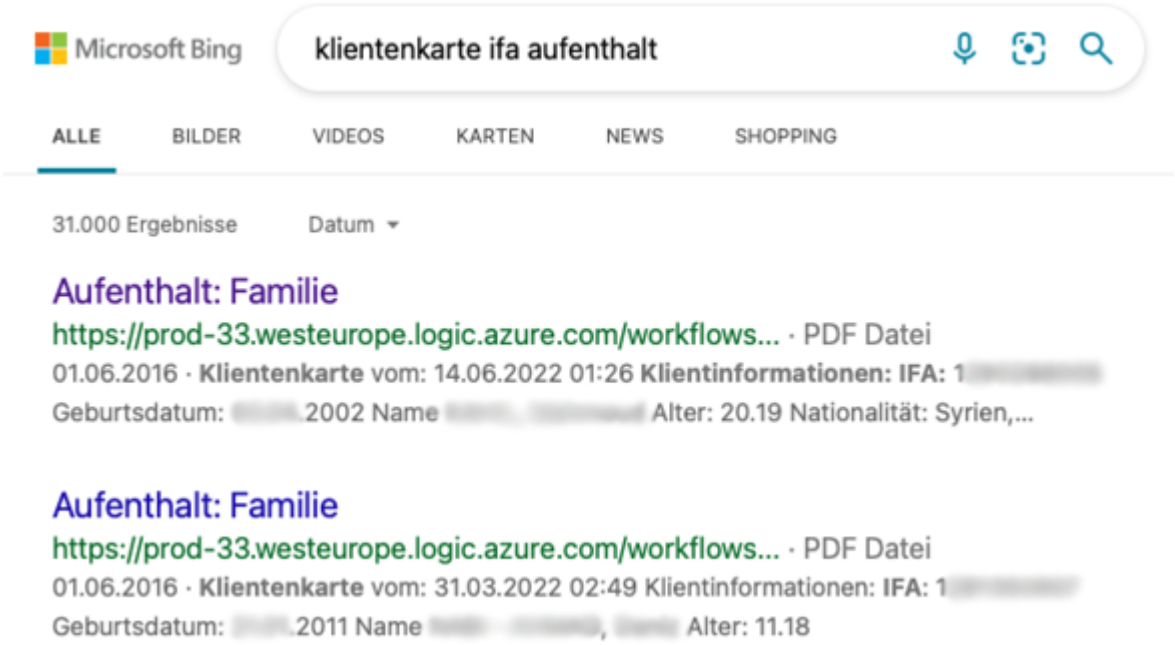
Von Jan Mahn

Das soll so nicht sein, dachte sich ein c’t-Leser Mitte Juni, als er in seiner bevorzugten Suchmaschine DuckDuckGo nach etwas ganz anderem gesucht hatte und die Suchergebnisse sah. In Kombination mit dem Suchwort „ifa“, unter dem man eher Treffer zur Funkausstellung in Berlin erwarten würde, fand er DIN-A4-Seiten im Querformat, betitelt mit „Klientenkarte“.

Die Bögen enthielten je ein Foto sowie diverse personenbezogene Daten wie Geburtsdatum, Sozialversicherungsnummer und Verwandtschaftsverhältnisse. Auch ein Bezug zum ursprünglichen Suchbegriff war vorhanden: Die Dokumente waren jeweils mit einer individuellen Nummer namens IFA versehen. Was es damit auf sich hatte, verrieten die Dokumente nicht. Unser Leser verfeinerte seine Suchanfrage und konnte DuckDuckGo sowie Microsofts Suchmaschine Bing (aus deren Daten sich auch DuckDuckGo bedient) dazu bringen, eine ganze Ergebnisseite mit solchen ominösen Klientenkarten auszuspucken. Mit diesen Erkenntnissen und der Suchanfrage wandte er sich an die c’t-Redaktion.

Wir konnten das Problem bestätigen und machten uns auf die Suche nach dem Verantwortlichen für diese offenbar nicht geplante Veröffentlichung. Doch es war gar nicht so einfach, einen Betreiber auszumachen. Wo eine IFA als eindeutige Nummer verwendet wird, konnten wir mit einer Websuche nicht

ergründen, und auch die Domain half nicht weiter: Die Klientenkarten lagen auf einer Subdomain von westeurope.logic.azure.com und waren Bestandteile von Microsofts Produkt „Azure Logic Apps“. Damit können Firmen und Behörden Arbeitsabläufe digitalisieren – Formulare, Freigabeprozesse, Listen und Auswertungen.



Waren nicht für die Öffentlichkeit bestimmt: Bei Bing tauchten Klientenkarten mit personenbezogenen Daten auf. Laut Domain waren sie Teil eines Workflows bei Microsoft Azure.
Vieles sprach dafür, dass irgendjemand seine Klienten über einen solchen Azure-Workflow verwaltet und die veröffentlichten A4-Dokumente ein End- oder Zwischenergebnis eines Verwaltungsprozesses sind. Ein Name des Betreibers war in der Azure-Adresse und in den Dokumenten nicht enthalten, wir mussten also weitersuchen.

Doch wer nennt seine Kunden schon „Klienten“, ein Anwalt vielleicht? Auffällig war die Nationalitäten der Klienten – vor allem Syrer und Afghanen. Das deutete darauf hin, dass es sich um ein Verfahren zur Registrierung von Geflüchteten handeln könnte. Also kontaktierten wir die für uns naheliegendste Adresse, das deutsche Bundesamt für Migration und Flüchtlinge. Vielleicht hatten wir eines ihrer Systeme gefunden. Und selbst wenn nicht, könnten sie vielleicht

immerhin verraten, was eine IFA-Nummer ist und zu welcher Organisation sie gehört.

Die Pressestelle des Bundesamtes meldete sich umgehend telefonisch und berichtete von einer eifrigen internen Suche nach der Herkunft der Datensätze. Das Fazit der Recherche: Aus Deutschland könnten die Datensätze sicher nicht stammen, das Bundesamt nutze keine Azure-Cloud-Produkte und auch eine zehnstellige Sozialversicherungsnummer auf den Dokumenten passe nicht nach Deutschland. Einen heißen Tipp hatte man doch für uns: Der Begriff „Klient“ und die Sozialversicherungsnummer könnten nach Österreich gehören. Die deutschsprachige Schweiz hatten wir zuvor bereits ausgeschlossen, weil die Dokumente ein ß enthielten, und so folgten wir der Spur nach Wien.

Spurensuche in Österreich

Unsere nächste Anfrage ging daher ans österreichische Bundesministerium für Inneres (BMI), dem das Bundesamt für Fremdenwesen und Asyl unterstellt ist. Volltreffer: Am nächsten Tag meldete sich der Pressesprecher telefonisch und bestätigte, dass man den Verursacher ausgemacht habe, und zwar die Bundesagentur für Betreuungs- und Unterstützungsleistungen (die BBU GmbH mit der Republik Österreich als einziger Gesellschafterin). Sie ist verantwortlich für die Betreuung und Beratung von Asylbewerbern und hat zur Registrierung ein Online-Verfahren auf Basis von Azure entwickeln lassen.

Nach unserem Hinweis begann das Unternehmen direkt mit der Fehlerbeseitigung und bestätigte uns später: „Wir haben von den einsehbaren Daten am Mittwoch, den 21. Juni 2022 um 09:40 Uhr erfahren und konnten diese Einsicht bereits am selben Tag um 10:18 Uhr schließen.“ Das deckt sich mit unseren Beobachtungen. Doch ein Problem blieb bestehen: Die Suchmaschinen Bing und DuckDuckGo zeigten die Treffer weiterhin an, auch wenn die verlinkten Seiten nicht mehr erreichbar waren. Und in der Vorschau der Suchergebnisse

standen ausgerechnet alle personenbezogenen Daten der Betroffenen als Fließtext hintereinander.

Am Telefon schilderte uns der Sprecher der BBU, was hinter den Kulissen passierte: Das Unternehmen, das den Azure-Workflow eingerichtet hatte, betreue noch andere Azure-Workflow-Kunden und stehe schon in Kontakt mit Microsoft. Kern der Untersuchung sei die Frage, ob es vielleicht ein generelles Problem gebe und über eine problematische Microsoft-interne Abkürzung massenhaft vertrauliche Links bei Microsofts Suchmaschine Bing landen. Eine Robots.txt-Datei, über die Suchmaschinen für gewöhnlich an Links kommen und die Seiten in den Index aufnehmen, konnte man nicht finden, auch keine anderen Anzeichen für systematisches Indexieren von Azure-Workflow-Links. Der Kontakt zu Microsoft war aber für ein anderes Problem nützlich: Die verwaisten Einträge im Bing-Suchindex verschwanden nach zwei Tagen spurlos. Für das Entfernen von Daten aus Suchmaschinenindexen ist das ein rasantes Tempo.

Arbeitshypothese

Einen grundsätzlichen Konfigurationsfehler konnten die Forschungen von BBU und der Microsoft-Partnerfirma nicht aufdecken, nur eine recht plausible Arbeitshypothese liefern. Die von der Suchmaschine verpetzten Links zeigten nicht nur eine Klientenkarte an, sie dienten auch als Trigger, um den nächsten Schritt im Registrierungsprozess anzustoßen. Eigentlich waren sie nicht dafür gedacht, im Browser geöffnet zu werden. Weil Mitarbeiter der BBU diese Schritte aber ab und zu per Hand auslösen mussten, könnten sie die Adressen, so die Theorie, manuell im Browser geöffnet haben – konkret in Microsoft Edge, dem Standardbrowser der BBU. Genau dieser Schritt könnte das Leck verursacht haben.

Wie wir nachstellen konnten, reicht ein einziges Zeichen vor dem https:// einer URL, und Edge interpretiert eine Eingabe in der Adresszeile nicht als URL, sondern als Suchanfrage für

Bing. Ein solches Zeichen ist beim händischen Kopieren und Einfügen schnell falsch kopiert und genug solcher Suchanfragen könnten Bing veranlassen, die eigentlich vertrauliche Adresse zu indexieren.

Kurzerhand probierten wir selbst, eine bisher garantiert von niemandem indexierte URL mit der Beschreibung eines eigens erfundenen Fantasietiers auf diesem Weg in den Bing-Index zu schleusen. Doch auch wiederholtes Suchen nach der URL mit mehreren Kollegen und verteilt über mehrere Tage konnte Bing nicht dazu bringen, die Seite zu indexieren. Die Arbeitshypothese der BBU, dass der Suchschlitz von Edge die undichte Stelle war, können wir damit weder bestätigen noch widerlegen; sie wirkt aber durchaus plausibel, weil nur Bing und nicht Google diese Daten fand.

Herausfinden konnten die Betreiber am Ende der Analyse, wie viele Datensätze betroffen waren: „Die anschließende Untersuchung durch ein internationales Expertenteam hat ergeben, dass aufgrund des spezifischen Verhaltens eines Workflows tatsächlich Daten von insgesamt 35 Asylsuchenden auf einigen Suchmaschinen zu finden waren. Für weitere Fälle wurden keine Indizien gefunden“, schrieb uns die BBU in ihrer abschließenden Stellungnahme. Die österreichische Datenschutzbehörde habe man über den Abfluss der Daten informiert.

Grundsatzproblem

Der Fall wirft ein Schlaglicht auf ein vielfach genutztes technisches Konzept und zeigt seine Schwächen auf: URLs, die etwas auslösen, Daten generieren oder anzeigen und die nur durch einen „geheimen“ Adressbestandteil geschützt sind, gibt es nicht nur bei Azure Logic Apps. Bei vielen Dateiablageplattformen einschließlich Nextcloud und Google Drive gibt es eine Möglichkeit, Links mit lesendem oder schreibendem Zugriff zu erzeugen und an andere zu verschicken.

Das Prinzip: Wer den Link kennt, darf zugreifen, man muss ihn also wie ein Geheimnis behandeln. Abgesichert ist das Konzept nur dadurch, dass der geheime Adressbestandteil ausreichend lang und zufällig generiert ist. Diese Bedingung gilt auch für die gefundenen Azure-Links, die nicht zu erraten waren.

Die Tücken lauern allerdings an vielen Stellen: Erste Schwachstelle ist der Mensch, der die vertraulichen Links vielleicht nicht allzu vertraulich behandelt. Sie werden (wie möglicherweise in diesem Fall) in Suchschlitze von Suchmaschinen eingetippt, an andere weitergeleitet, in cloudsynchronisierten Lesezeichenlisten gespeichert oder aus Bequemlichkeit aus der Firma ans private Mobiltelefon geschickt. Außerdem landen sie im Verlauf von Browsern und in Caches und können dort schlimmstenfalls von Unbefugten gelesen werden. Kurzum: Mit Links stellen viele Nutzer Dinge an, die sie mit ihren Passwörtern eher nicht machen würden.

Was tun?

Sollte man Adressen mit integrierten Geheimnissen also verteufeln und sich für ihre Ächtung einsetzen? Ganz so drastisch muss man vielleicht nicht vorgehen. Wer als Admin oder Entwickler Software mit solchen URLs bereitstellt, sollte aber gut abwägen, ob es sicherere Alternativen gibt und diesen den Vorzug geben. Sofern möglich sollten Abfragen immer nur nach Anmeldung mit Benutzername und Passwort gelingen, am besten abgesichert mit einem zweiten Faktor. Sobald personenbezogene Daten im Spiel sind, ist deren Schutz wichtiger als der Komfortgewinn durch eine gesparte Anmeldung.

Auch aus dem Grundschutz-Kompendium des BSI (siehe ct.de/y8ct) kann man eine Pflicht ableiten, solche URLs mit Geheimnissen durch eine Benutzeranmeldung zu ersetzen. Im Abschnitt ORP.4 zu „Identitäts- und Berechtigungsmanagement“ heißt es: „Der Zugang zu schützenswerten Ressourcen einer Institution ist auf berechtigte Benutzer und berechtigte IT-Komponenten einzuschränken. Benutzer und IT-Komponenten müssen

zweifelsfrei identifiziert und authentisiert werden.“ Mit anonymen Links, die womöglich von mehreren Mitarbeitern genutzt und fleißig umher kopiert werden, ist das definitiv nicht gewährleistet.

Wenn für eine Anwendung wirklich nur eine solche „geheime“ URL infrage kommt, kann man das Risiko für Missbrauch immerhin dadurch minimieren, dass man die Links nur in dem überschaubaren Zeitfenster funktionieren lässt, in dem sie unbedingt gebraucht werden – und keine Minute länger. (*jam@ct.de*)

BSI-Grundschutzkompendium: ct.de/y8ct