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.

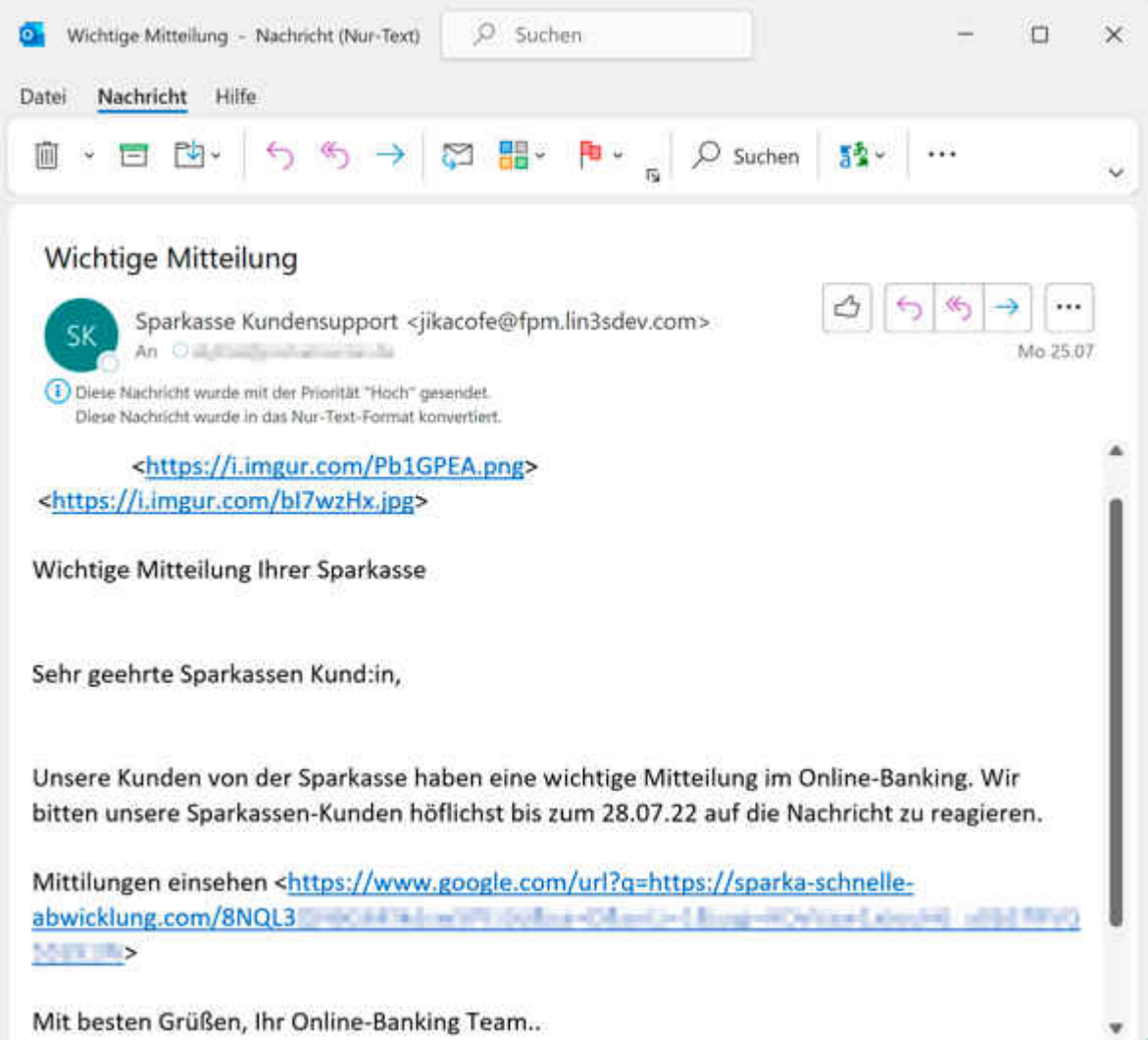
Mit den folgenden Strategien und Tipps sind Sie dazu in der Lage, verdächtige Mails zu erkennen und die richtigen Entscheidungen zu treffen, um nicht in die Phishing-Falle zu tappen. Es geht mit den offensichtlichen Warnsignalen los, die jeder kennen sollte, und weiter damit, wie Sie anhand der Mail-Innereien 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.

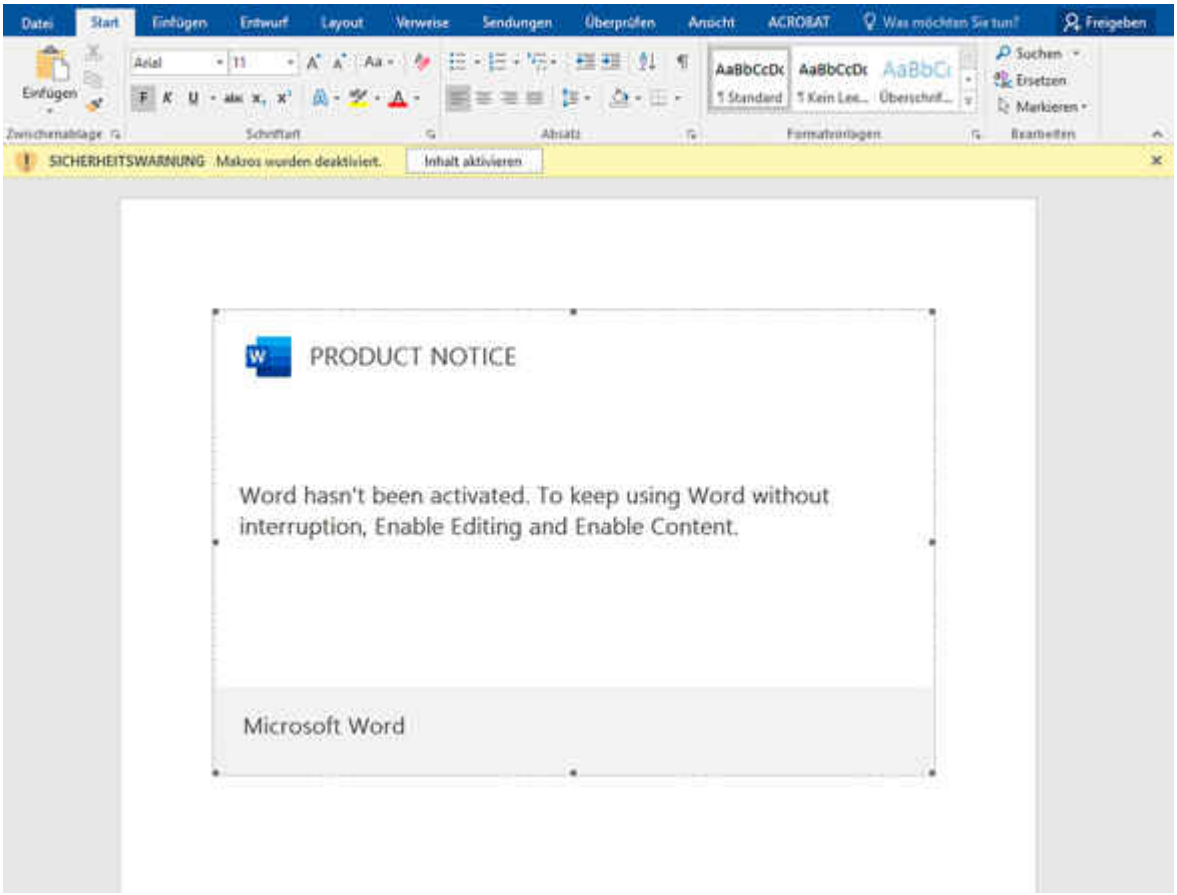
Gelegentlich verwickeln Sie die Betrüger auch in ein Gespräch, um zunächst eine Vertrauensbasis aufzubauen, ehe es ans Eingemachte geht. Geht es ums Geld, sollten den angegebenen Zahlungsempfänger genau überprüfen. Passen die angegebenen Bankdaten tatsächlich zu dem Unternehmen, das die Rechnung ausgestellt 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.



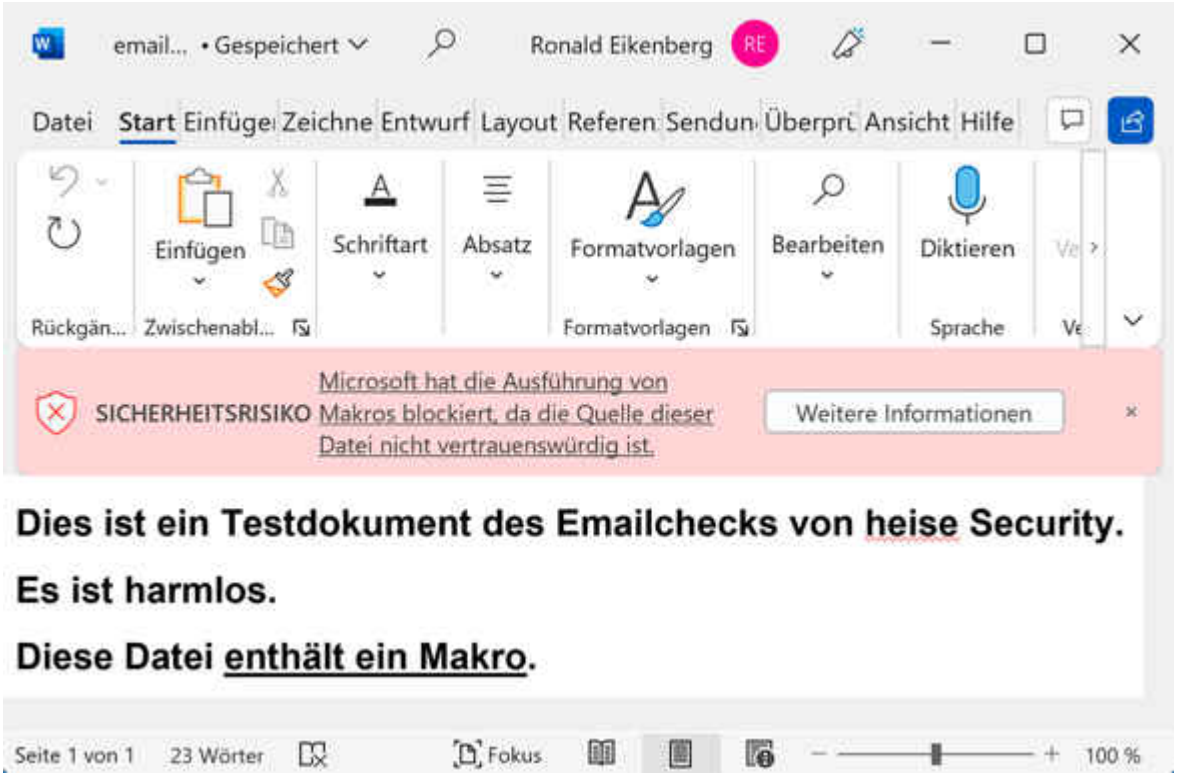
Phishing-Dokumente fordern häufig mit fadenscheinigen Argumenten dazu auf, auf die gelbe Leiste von Microsoft Office zu klicken. Dadurch wird das mitgelieferte Schadcode-Makro ausgeführt.
Kontrollieren Sie die Makro-Einstellungen in Ihrem Office, um sicherzustellen, dass Makros nicht automatisch ausgeführt 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.

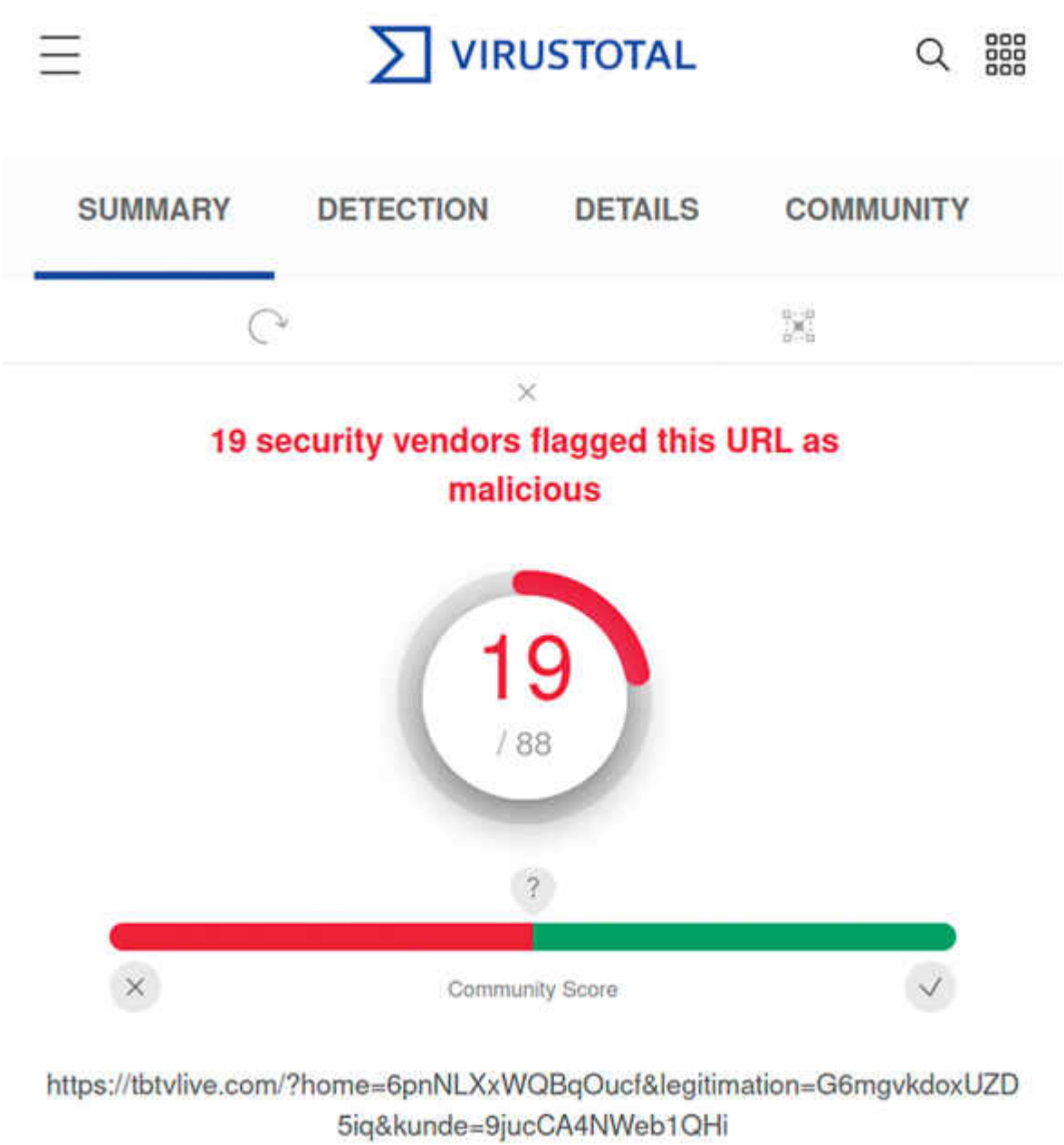
Wichtig zu wissen ist, dass die Office-Formate DOCX, PPTX und XLSX keine Makros enthalten können, von solchen Dokumenten geht also eine geringere Gefahr aus. Eine Unbedenklichkeitserklärung ist das jedoch nicht, denn selbst ohne Makros sind Angriffe möglich, zum Beispiel durch Sicherheitslücken in Office. 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

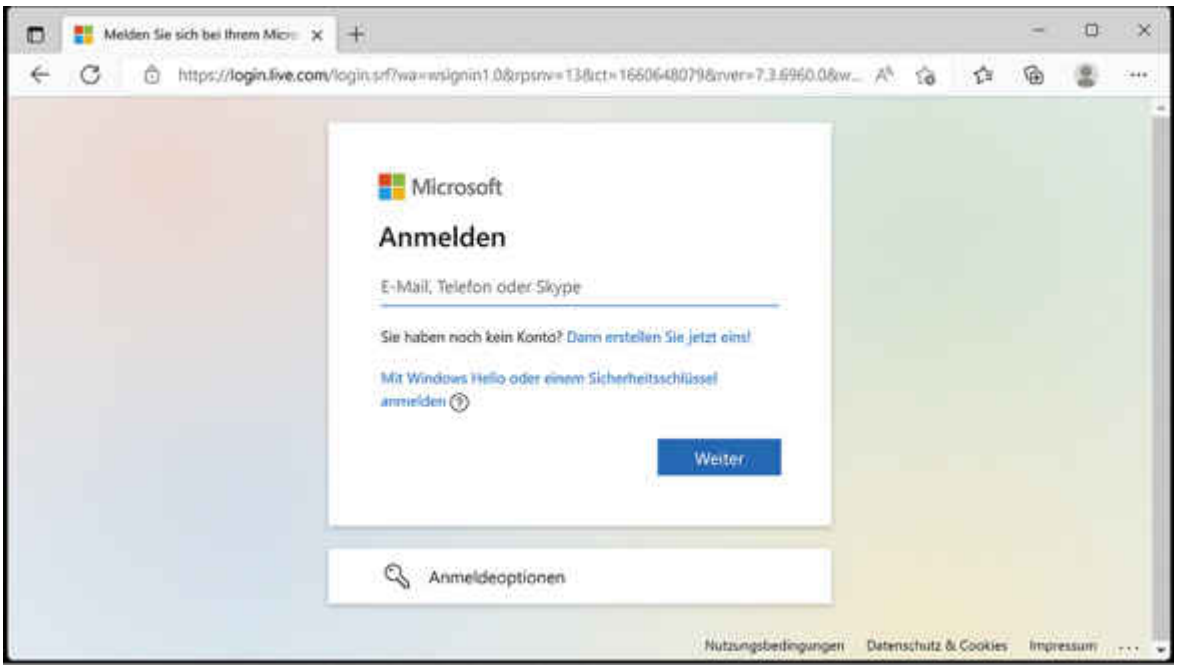
Nicht nur Dateianhänge können gefährlich sein, sondern auch Links. Stellen Sie wie oben beschrieben den Nur-Text-Modus im Mail-Client ein, damit man Ihnen keine manipulierten Links unterjubeln kann, deren Ziel von der angezeigten URL abweicht. Achten Sie außerdem darauf, dass die Zieladresse mit https://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

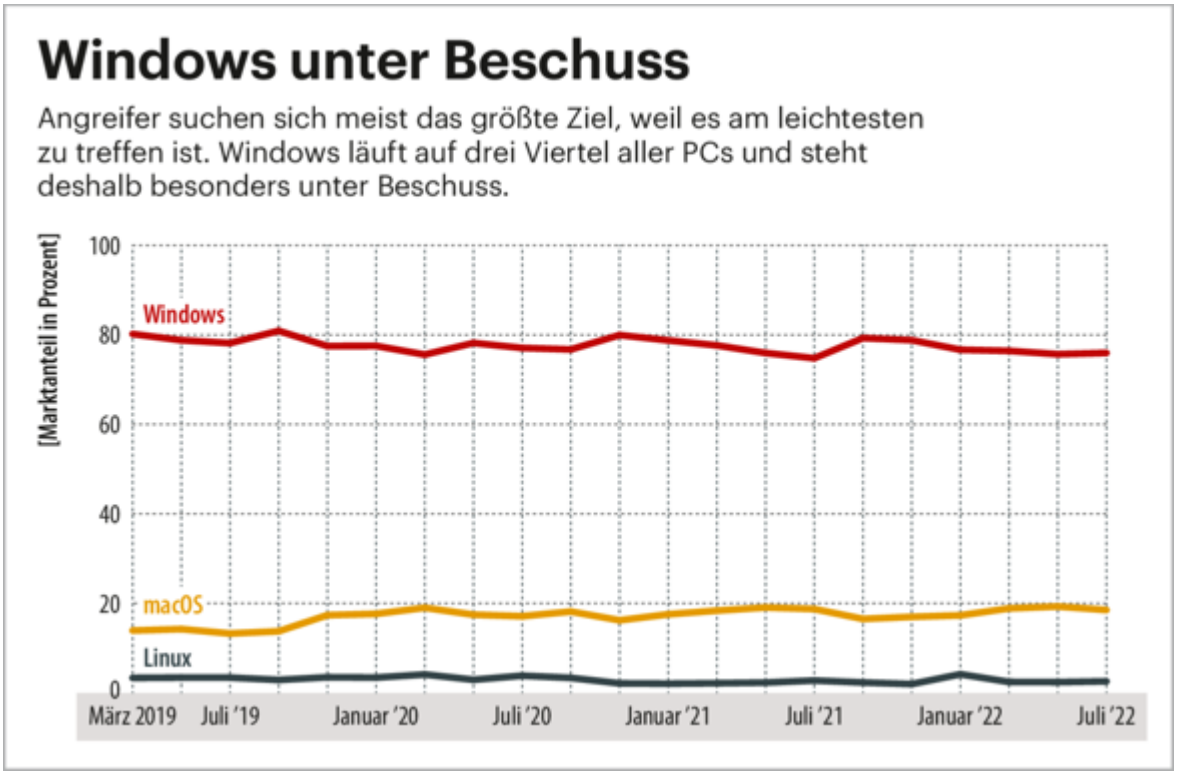
Haben Sie Ihre Zugangsdaten versehentlich einer Phishing-Website anvertraut, schauen die Cyber-Ganoven dann trotzdem in die Röhre, da sie sich ohne den zweiten Faktor nicht einloggen können. Gefährlich wird es allerdings, wenn Sie nicht nur Ihre Zugangsdaten, sondern auch das Einmalpasswort in die Phishingsite 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.

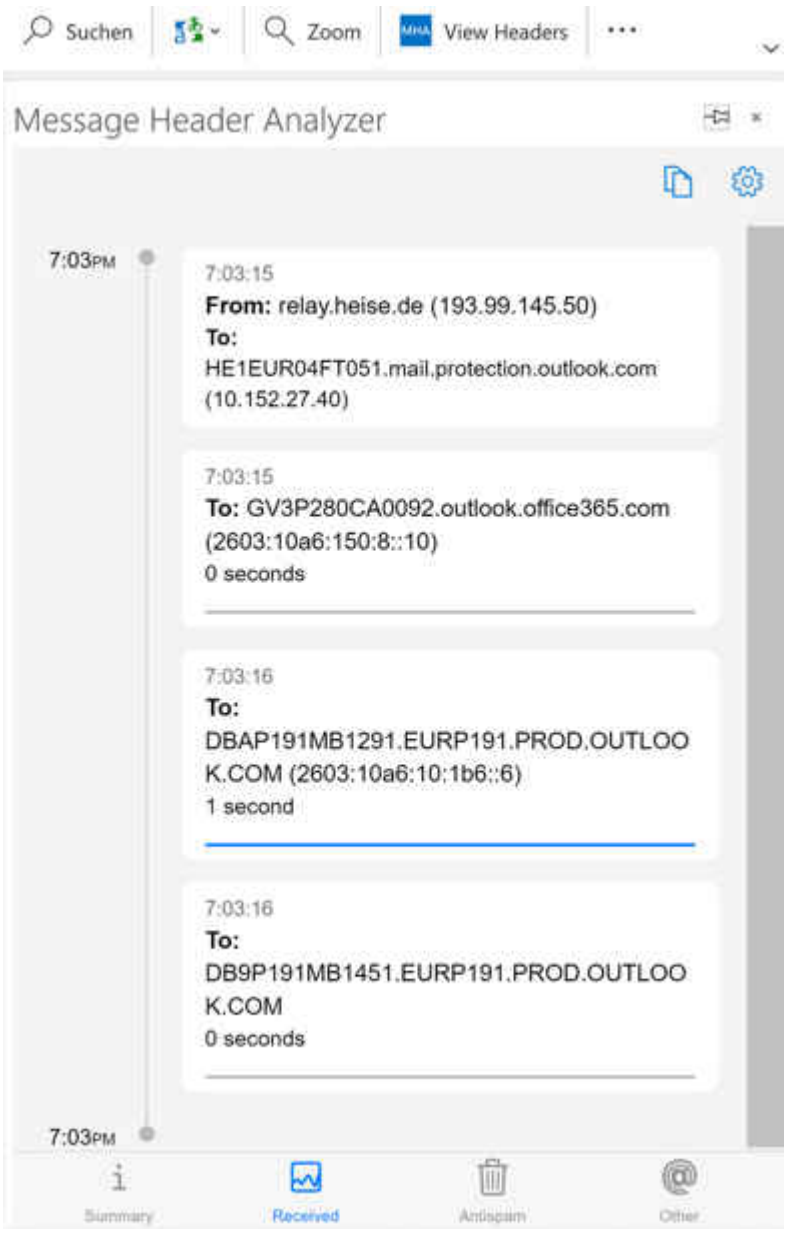
Achten Sie auch auf verdächtige Nachrichten aus sämtlichen Kanälen: Nicht nur Mails, auch WhatsApp-Nachrichten, SMS, Social Networks wie Facebook und Instagram, Anrufe und so weiter werden für Phishing missbraucht. Haben die Angreifer Kontaktdaten kopiert, kommt die Phishing-Nachricht womöglich sogar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

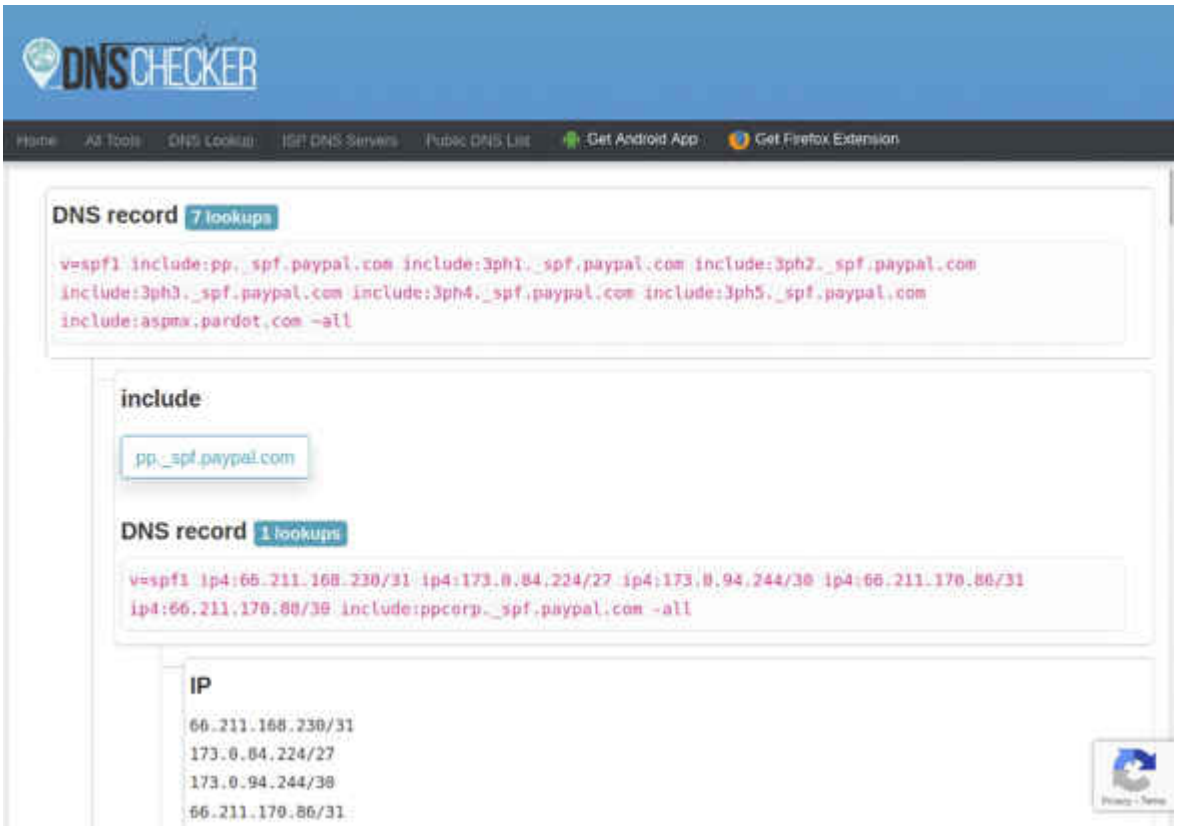
Anti-Spoofing-Check

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