Anleitung zur Abwehr von Spyware, Dialern und Spam-Emails

Benutzeranleitung

Inhaltsverzeichnis

Inhaltsverzeichnis

Autoren

Spyware

Autor: Grigory Pavlov

Spam Email & Dialern

Autor: Colin van Loo

Spyware

Was ist Spyware?

Sogenannte "Spyware" (vom engl. ***spy*** (Spion) + ware) ist Software, deren Absicht es ist, Informationen über eine Person oder Organisation zu sammeln und diese Informationen an eine Drittpartei, meistens den Hersteller der Software, zurückzusenden. Dieses Verhalten kann sowohl in Malware als auch in vertrauenswürdiger Software vorhanden sein. Auch Webseiten können Spyware-Verhalten aufweisen, wie zum Beispiel Web-Tracking.

Erkennen von Spyware

Da es verschiedene Arten von Spyware gibt, ist es schwierig, definitive Indikatoren niederzulegen, jedoch kommen folgende Symptome oft vor:

- erhöhte CPU-/RAM-Nutzung, deutlich höher als von offenen Applikationen gebraucht
- unerklärliche Netzwerkaktivität
- Antivirus (falls installiert) zeigt Warnungen
- es werden Programme ohne Einwilligung des Nutzers installiert, modifiziert oder deinstalliert
- "Browser Hijacking": Browser läuft langsamer, Standardsuchmaschine wurde geändert, verdächtige Extensions, Werbe-Pop-Ups

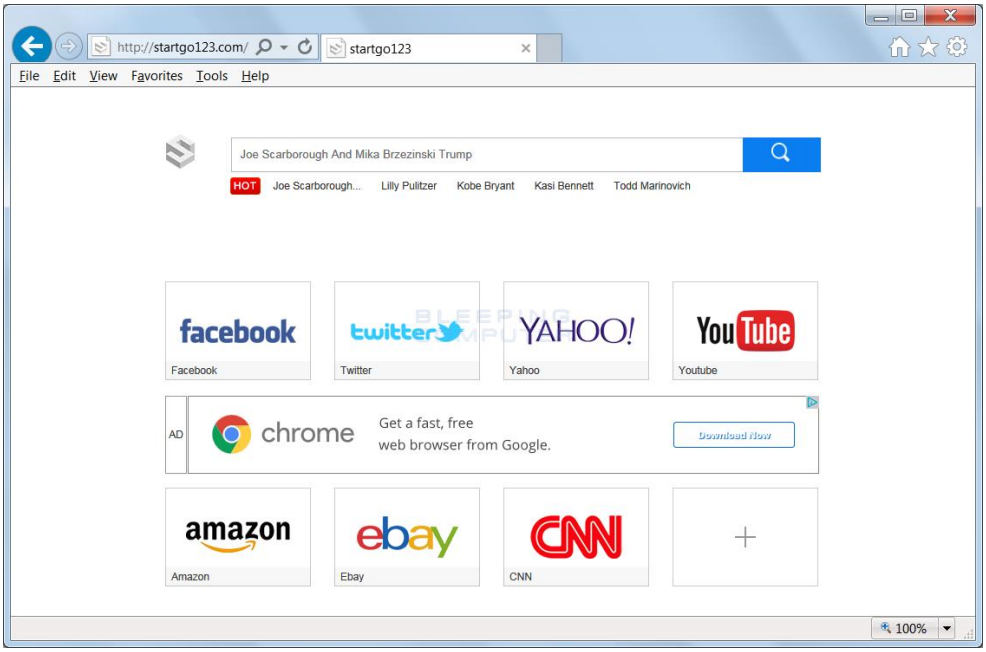

Abbildung 1: Browser eines mit Spyware infizierten Geräts nach Hijacking

Präventiv gegen Spyware vorgehen

Man kann verschieden gegen Spyware oder Malware (Schadsoftware) allgemein vorgehen. Beispielsweise gibt es spezielle Anti-Spyware-Applikationen mit Echtzeitschutz:

- Norton 360
- Bitdefender
- TotalAV
- ClamAV (Open Source)
- ...viele andere

Zu beachten ist jedoch, dass auch sogenannte "Trüge-Anti-Virusprogramme" im Umlauf sind. Falls Sie unsicher sind, überprüfen sie zuerst auf einem anderen Gerät via das Internet, ob der Antivirus auch wirklich einer ist.

Ausserdem kann seitens Nutzer das Verhalten an die Möglichkeit einer Infizierung angepasst werden. Solches sollte man vermeiden:

- deaktivieren des Antivirus-Programms zur Installation eines Programms
- veralteter Browser oder Windows-Version (die meiste Spyware ist auf Windows-Systeme vorbereitet)
- neuen, unbekannte Applikationen mit Adminrechten ausführen

Zusätzlich kann eine Firewall oder ein Werbeblocker wie uBlock eingerichtet werden, um Netzwerkverkehr zu filtern.

Spyware effektiv entfernen

Falls die präventiven Massnahmen nicht eingesetzt wurden, kann man versuchen, so gut wie möglich Spyware vom Gerät zu entfernen:

1. Einen Malware-Scanner installieren (falls möglich via anderes Gerät herunterladen)
2. jegliche Internet-Verbindung (per Kabel oder WLAN) trennen um weiteren Schaden zu vermeiden
3. PC neustarten
4. Schnellstmöglich einen Scan durchführen
5. weiteren Anweisungen des Malware-Scanners folgen

Spam Emails

Worauf achten?

Im Buch «Thinking, Fast and Slow» von Daniel Kahneman, werden zwei Denk-Systeme beschrieben. Das erste ist schnell, automatisch und unbewusst, das zweite schlau, logisch und methodisch.

Das erste System ist aktiv bei Langeweile, wenn man wie immer Handelt (Gewohnheit) und auch bei Angst, wenn man schnell handeln muss.

Die grösste Zeit ist System 1 aktiv. Dieses System kümmert sich nicht darum, jede E-Mail genau unter die Lupe zu nehmen.

Deswegen zielen es Angreifer meistens auf das erste System ab. Wenn Leuten erklärt wird, vorauf sie bei Phishing-Attacken zu achten haben, ist das vernünftige zweite System aktiv. Wenn Sie dann aber eine richtige Phishing-E-Mail erhalten und System 1 reagiert, war das ganze Lernen umsonst.

Es hat somit einen viel grösseren Effekt, in einer Firma die Angestellten zu testen und denen, die darauf reingefallen sind zu erklären, was sie falsch gemacht haben. Auch hält die Wirkung nicht für immer an, Firmen sollten immer wieder sogenannte «Pen-Tests» durchführen.

Ironischerweise ist eine Anleitung wie diese hier also von eher geringem Nutzen, wenn man das hier gelernte nicht auch direkt in der Praxis anwenden kann.

Absender

Es gibt zwar Möglichkeiten, den Absender zu fälschen, allerdings wird der Angreifer in den meisten Fällen eine einfache E-Mail nutzen, mit einer Domäne die sich möglichst authentisch anhört. Die Adresse beinhaltet vielleicht den Namen einer Bekannten Firma wie Microsoft, um Vertrauenswürdiger zu erscheinen. Ein beliebter Trick ist es auch, ein «I» (grosses i) durch ein «l» (kleines L) zu ersetzen. Ein weiterer Trick tauscht einzelne Buchstaben durch identisch aussehende, spezielle Unicode-Zeichen aus.

Notfalls kann man die Adresse mit einem «ASCII-Validator» prüfen lassen, um sicherzustellen, dass nur gewöhnliche ASCII-Buchstaben in ihr enthalten sind.

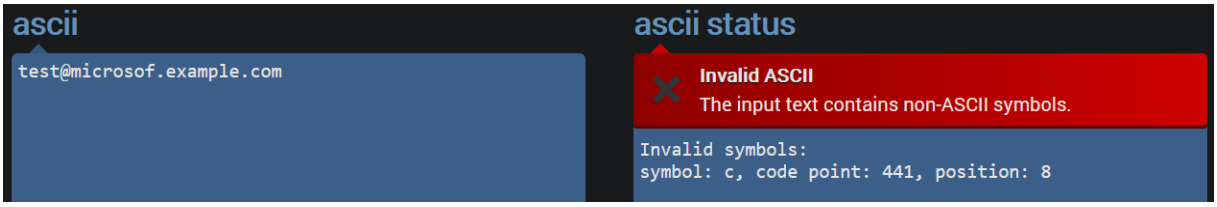

Abbildung 2: Der Buchstabe "c" wurde durch das kyrillische Symbol "Es" ersetzt.

Wichtig ist auch, auf die Domäne zu achten. Bei der Adresse «microsoft.example.com» ist die Domäne «example.com», also nicht Microsoft. Alles davor ist lediglich eine Sub-Domäne welche frei gewählt werden kann.

Links

Seien Sie besonders vorsichtig vor Links in E-Mails. Auch hier können URLs oft andere imitieren indem «l» mit «I» ersetzt, oder kyrillische Buchstaben verwendet werden.

Passwortmanager mit Browser-Erweiterungen können sich hier auch als ganz nützlich erweisen. Nehmen wir an, ein Link in einer E-Mail die angeblich von PayPal stammt, führt uns zu einer Webseite, die genau gleich aussieht wie die Login-Seite von PayPal (Es ist trivial einfach, eine Webseite zu kopieren). Ein Nutzer würde vielleicht einfach sein Passwort eingeben. Der Passwortmanager stattdessen erkennt sofort, dass die URL nicht übereinstimmt und wird kein Passwort vorschlagen.

Anhänge

Öffnen Sie niemals Anhänge von unbekannten Absendern. Öffnen Sie nur dann einen Anhang, wenn Sie diesen auch erwartet haben.

Achten Sie bei Dateien unbedingt auf das Dateiformat. Microsofts Windows 10 versteckt leider die Dateiendungen standardmässig. Um Windows zu sagen, dass Sie die Dateiendungen angezeigt haben möchten, müssen Sie zuerst den «Datei Explorer» starten.

1. Klicken Sie oben Links auf «File».
2. Klicke Sie auf «Options».
3. Navigieren Sie zum «View»-Reiter.
4. Entfernen Sie das Häkchen bei «Hide extensions for known file types».
5. Bestätigen Sie mit Klicken auf «Apply».

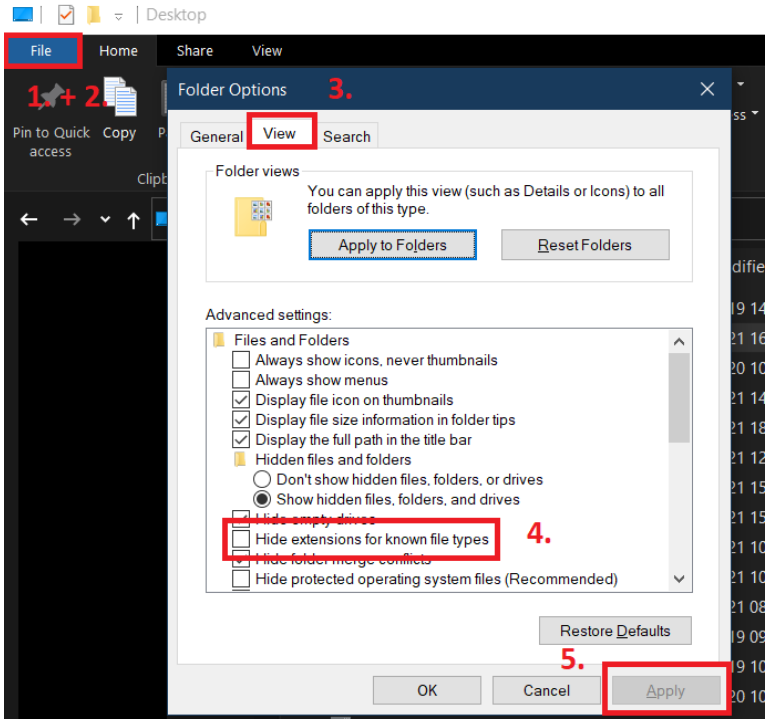

Abbildung 3: Dateiendungen Anzeigen

Generell gilt, dass Microsoft Office-Dateien wessen Dateityp nicht mit einem «x» enden unsicher sind. Also «.docx» und «.xlsx» sind sicherer als «.doc» und «.xls».

Dateien ohne dem «x» können nämlich Makros beinhalten. Wird eine solche Datei geöffnet, kann Schadsoftware auf dem Computer installiert werden. Sollte Microsoft Word beim Öffnen einer Datei eine Warnmeldung bezüglich «Makros/Inhalte aktivieren» anzeigen, sollten Sie dort niemals mit «Ja» bestätigen.

Viele Nutzer haben die Eigenschaft, immer auf den grössten Knopf drücken zu müssen. Dies wird auch sehr gerne von Betrügern ausgenutzt. Im Beispiel von Microsoft Word, wird der «Enable Content»-Button gross angezeigt. Das «x» zum Schliessen der Warnung ist ganz klein versteckt, es fällt einem fast nicht auf.

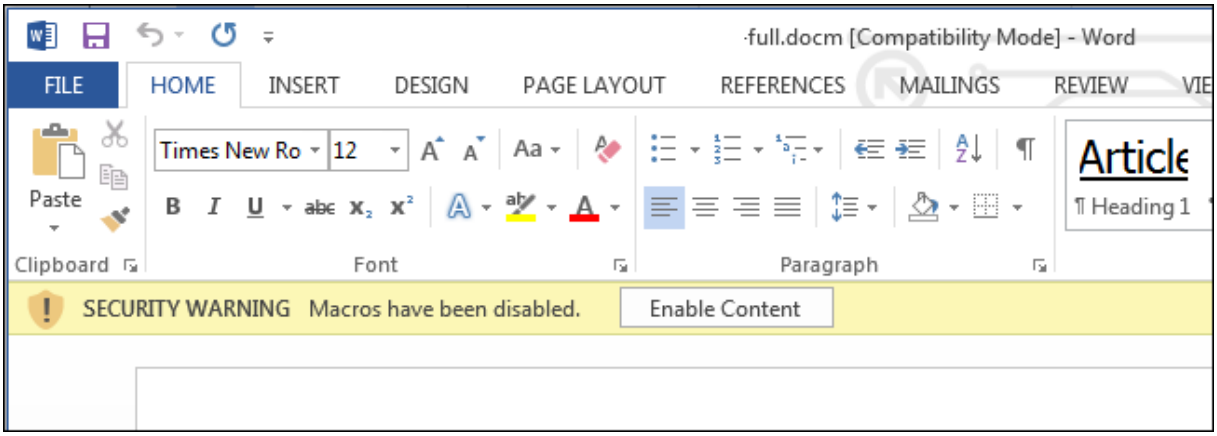

Abbildung 4: "Enable Content" ist ein gefährlicher Knopf

Falls es für die Firma trotzdem wichtig ist, Makros zu nutzen, können diese übrigens signiert werden, sodass nur «vertraute» Makros ausgeführt werden können.

Innerhalb / Ausserhalb

Manche Firmen zeigen eine Warnmeldung an, wenn die E-Mail von ausserhalb der Organisation gesendet wurde.

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and you expect to receive a link or attachment from them.

Abbildung 5: Diese E-Mail stammt von ausserhalb der Organisation

Dringlichkeit

Wie bereits im Kapitel «Worauf achten?» erklärt, haben es Angreifer meistens auf System 1 abgesehen. Deshalb rufen Spam-E-Mails oft zur Dringlichkeit auf, um dafür zu sorgen, dass das erste System (Angst, schnell handeln) aktiv wird.

Seien Sie also besonders vorsichtig vor dringlichen E-Mails und handeln Sie nicht unüberlegt.

Sprache

Achten Sie darauf, wie eine E-Mail geschrieben ist. Kommen viele Rechtschreibfehler vor? Wie ist die Formulierung?

Reply-to

Sollte ein Absender gefälscht sein, wird die E-Mail oft so konfiguriert, dass bei Klicken auf «Antworten» automatisch in dem «Antworten an»-Feld eine andere Adresse erscheint.

Der Angreifer ist schliesslich nicht wirklich in Besitz der vorgegebenen Domäne und somit auch nicht in der Lage, Antworten zu empfangen, da diese stattdessen an den richtigen Besitzer gehen würden.

Achten Sie also darauf, dass die Absender und «Antworten an» Andressen übereinstimmen. Es gibt natürlich auch völlig legitime Gründe, diese Funktion zu nutzen, ein eindeutiger Hinweis auf einen Phishing-Versuch ist dies nicht.

Send via / Signed by

Gewisse E-Mail-Clients zeigen manchmal so etwas in der Form von «jemand@email.com via etwas.com» an. Dies bedeutet, dass die Domäne, die die E-Mail gesendet hat (etwas.com) nicht mit der Domäne in der E-Mail-Adresse (email.com) übereinstimmt. Dies kann in vielen Fällen legitime Gründe haben, könnte aber auch ein Hinweis darauf sein, dass der Absender gefälscht wurde.

Sicherheits-Tests

Es gibt verschiedene Tests die E-Mail-Clients automatisch durchführen können, um die Authentizität einer Mail zu prüfen. Viele Clients verstecken diese Funktion allerdings vor dem Nutzer und machen es schwer, diese zu finden.

Die meisten E-Mail-Clients werden wahrscheinlich dem Nutzer die Möglichkeit bieten, die E-Mail-Headers anzusehen.

Headers in Outlook

Öffnen Sie die E-Mail mit einem Doppelklick. (Ganz, nicht nur in der Vorschau.)

1. Klicken Sie auf «File»
2. Klicken Sie auf «Properties»

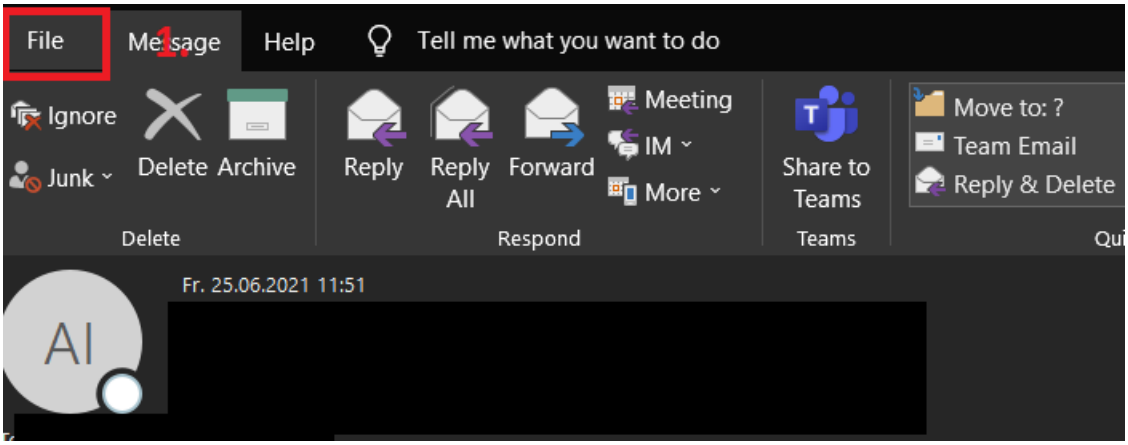

Abbildung 6: Drücken Sie auf "File"

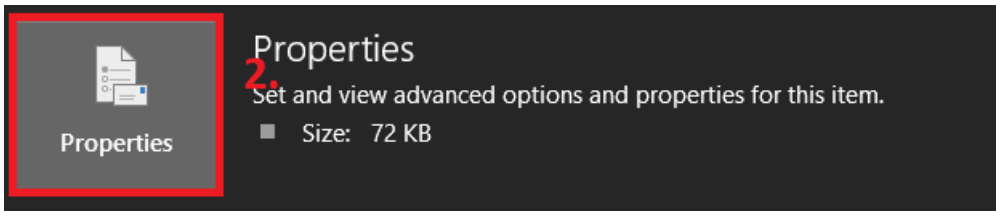

Abbildung 7: Klicken Sie auf "Properties"

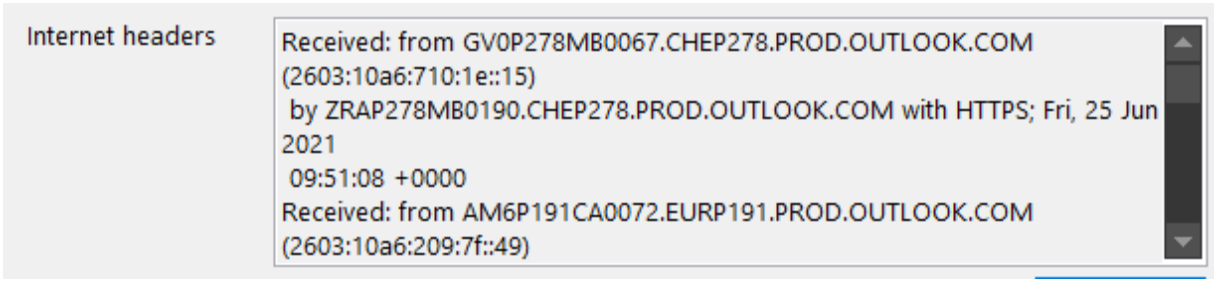

Abbildung 8: Werfen Sie einen Blick auf die "Internet Headers"

Headers in Protonmail

1. Klicken Sie auf «More»
2. Klicken Sie auf «View Headers»

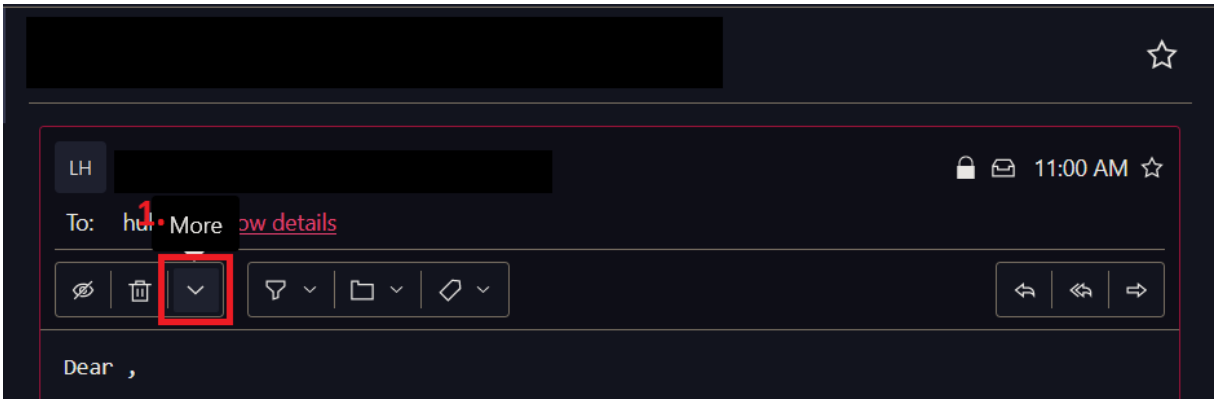

Abbildung 9: Klicken Sie auf "More"

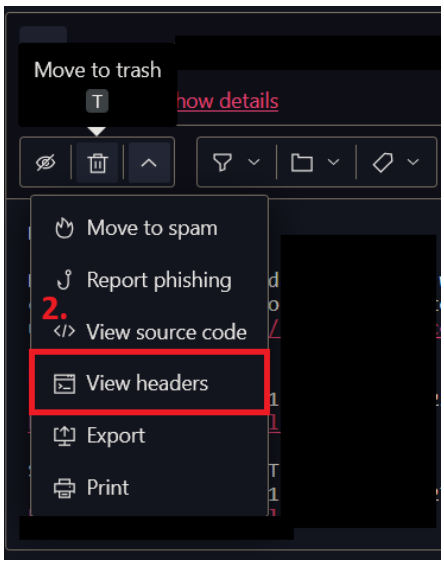

Abbildung 10: Klicken Sie auf "View Headers"

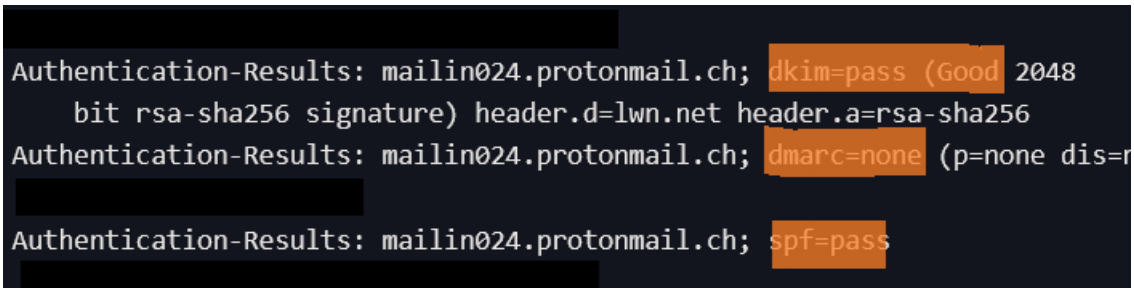

Abbildung 11: Headers, die wichtigen Tests wurden hier markiert.

SPF, DKIM und DMARC

Sofern der Absender diese «Authentication Headers» korrekt aufgesetzt hat, können diese genutzt werden, um zu bestätigen, dass die E-Mail tatsächlich von ihm kommt und nicht gefälscht wurde. Sollte einer oder mehrere dieser Checks fehlschlagen, ist es ziemlich sicher eine Fälschung.

Dies bestätigt lediglich, ob die E-Mail wirklich von der vorgegebenen Domäne stammt und unterwegs nicht verändert wurde, **nicht aber ob es Spam ist.**

SPF

Verifiziert, dass der Server der die E-Mail sendet, auch dazu autorisiert ist. Dies ist sehr einfach zu umgehen, deshalb sollet man sich nicht zu sehr darauf verlassen. Sollte dieser Check fehlschlagen (NEUTRAL/SOFT FAIL/FAIL), bedeutet dies sicherlich nichts Gutes.

DKIM

Verifiziert, dass die E-Mail nicht «unterwegs» verändert wurde und von der vorgegebenen Person geschrieben worden ist. Dabei ist wichtig, nicht nur zu achten, ob der Test erfolgreich war, aber auch von welcher Domäne der Test durchgeführt worden ist. Die Domäne sollte mit der Adresse des Absenders übereinstimmen.

War der Test erfolgreich, aber die Domänen stimmen nicht überein, bedeutet dies, dass ein valides Zertifikat gesendet wurde, allerdings von einer anderen Domäne. In diesem Fall erscheint auch das «via».

DMARC

Dies ist genau worauf DMARC testet: Stimmt das Zertifikat und die Domäne, die das Zertifikat sendet, mit dem Absender überein?

Spam melden

Um weiteren Befall zu vermeiden, ist es wichtig, dass eine Spam-E-Mail bei Erhalt sofort der zuständigen Abteilung gemeldet wird. Um dies zu vereinfachen haben Firmen dazu die Möglichkeit, einen «Spam-Melde-Button» in Outlook einzubauen.

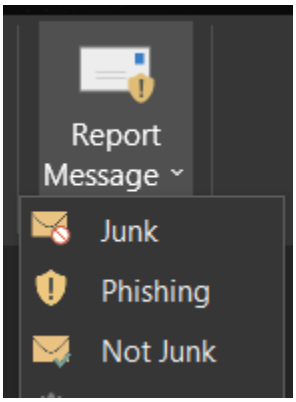

Abbildung 12: Spam-Melde-Button

Dialern

Vhishing, kurz für Voice Phishing, beschreiben Spam Angriffe über das Telefon. Angreifer nutzen häufig «Voice over IP» (VoIP) und Techniken wie «Caller-ID-Spoofing» um unentdeckt zu bleiben.

Der Betrüger gibt sich als ein Mitarbeiter einer Firma, zum Beispiel einer Bank, der Polizei, Telefon oder Internet Anbieter aus und versucht persönliche Daten zu erlangen, wie Kreditkartendetails oder andere vertrauliche Informationen.

Dringlichkeit & Autorität

Auch beim Vhishing wird oft die Dringlichkeit als Mittel genutzt, um jemanden zu täuschen. Der Betrüger gibt sich zudem oft als jemand in einer hohen Position aus. Mitarbeiter sind normalerweise sehr Hilfsbereit, vor allem wenn ein Vorgesetzter etwas von ihnen verlangt.

Tech Support

Sehr verbreitet sind auch Tech-Support-Scams. Zum Teil werden Webseiten genutzt, die dem Besucher eine Meldung anzeigen, dass er einen Virus hätte und einer bestimmten Nummer anrufen sollte, die angeblich zu Microsofts Kundendienst gehört.

Das Ziel dieser Betrüge sind ältere Leute, welche oft darauf reinfallen und dann der Nummer anrufen.

Anrufer-ID fälschen

Die Anrufer-ID kann einfach gefälscht werden, man sollte sich also nicht darauf verlassen.

Abbildung 13: Die Anrufer-ID kann leicht gefälscht werden

Zurückrufen

Geben Sie niemals wichtige und persönliche Daten über das Telefon aus. Sollten Sie einen Anruf erhalten, der Ihnen wichtig und authentisch erscheint, teilen Sie dem Anrufer mit, Sie würden zurückrufen. Suchen Sie dann auf der Webseite nach einer Kontaktnummer und rufen Sie diese stattdessen an.

Quellenverzeichnis

Quellen

Browser Hijacking: https://en.wikipedia.org/wiki/Browser_hijacking 5
Dialern: The Art of Deception - Buch von Kevin D. Mitnick 13
Extensions: https://developer.chrome.com/docs/extensions/ 5
Spyware: pcmag.com - Windows Computers Were Targets of 83% of All Malware Attacks in Q1 2020 5
Thinking, Fast and Slow: Buch von Daniel Kahnemann 7
uBlock: https://ublockorigin.com/ 6