Lüscher, Chatzimichalis

Abwehr von Spyware, Dialern und Spam-Emails

25. März, 2020

Allgemein

In dieser umfangreicher Benutzeranleitung wird die Handhabung und Massnahmen benannt, die man zur Abwehr von Spyware, Dialer und Spam-mails ergreifen kann.

Spyware

Spionageprogramme, die man sich vielleicht unbewusst zusammen mit einem Software-Download ins Haus geholt hat, nisten sich in Windows ein, bombardieren Anwender mit personalisierter Bannerwerbung und stehlen im schlimmsten Fall Daten. Ohne spezielle Hilfsprogramme haben selbst Betriebssystemkenner kaum Chancen, dieser raffiniert getarnten Spyware auf die Schliche zu kommen.

Wie kann ich mich im Internet sowie auch lokal dagegen schützen?

Ein guter Anfang ist die Verwendung einer Firewall (Theorie dazu findet man hier) sowie der Einsatz spezieller Tools gegen Spyware, wie **Ad-aware, AntiSpyware, AntiSpion, Bazooka Spyware Scanner, PestPatrol, Spy Sweeper, Spybot S&D**, und letztlich der standardmässigen

Windows Defender, der bei allen Tests relativ gut abschneiden tut und somit für euren Privatgebrauch genügt. Wie beim Virenschutz gilt auch hier, dass die Software regelmässig auf den aktuellen Stand gebracht werden muss.

Wie merke ich, ob ich mein Rechner von Spyware schon infiziert ist?

Ein Computer könnte infiziert sein, wenn eines oder mehrere der folgenden Symptome auftreten:

- Der Computer funktioniert aussergewöhnlich langsam, besonders beim Surfen im Web.
- Der Webbrowser öffnet Werbefenster, die in keinem erkennbaren Zusammenhang zu den besuchten Websites stehen.
- Die Startseite oder Suchmaschine des Webbrowsers wurde geändert, wechselt bei Änderungen automatisch wieder auf diese Einstellung.
- Im Lesezeichen- bzw. Favoritenmenü befinden sich neue Einträge, die nicht vom Benutzer gespeichert wurden.
- Der Computer verbindet sich selbständig mit dem Internet.
- Die Firewall meldet laufend Versuche von Programmen, die eine Verbindung zum Internet herstellen wollen.
- Es befindet sich eine Spyware-Warnung auf dem Desktop als Hintergrundbild, die zum Beispiel den Erwerb eines vorgeblichen Anti-Spyware-Programms bewirbt

Merkmale

Die Kombination von Informationen aus Spyware mit Nutzerdaten, die zum Beispiel während einer Softwareregistrierung eingegeben werden, lässt mit jedem Seitenaufruf im Web ein immer genaueres Verbraucherprofil entstehen. Es ist daher ratsam, die Vorteile und Risiken bei allen Softwaredownloads sorgfältig gegeneinander abzuwägen. Und auch bei kommerzieller Software solltet Ihr die Lizenzbestimmungen kritisch daraufhin zu prüfen, ob die dort vereinbarte Verwendung von Nutzer- und Gerätedaten tatsächlich für einen störungsfreien Gebrauch der betreffenden Anwendung notwendig ist. Einen Beispiel, wie zugänglich und einfach es ist solche Spyware auf einem global verbreiteten Store zu haben, zeigt sich folgendes Beispiel:

Schnüffelsoftware jahrelang im App-Store verborgen

Im April 2017 entdeckten Sicherheitsforscher eine Spyware-App, die unter dem Namen "**System Update**" bereits seit 2014 im US-amerikanischen Google Play App-Store zum Download zur Verfügung stand. Wer das vermeintliche Update auf sein mobiles Gerät lud, erhielt nur die Nachricht, dass der Update-Versuch gescheitert sei. Den Sicherheitsforschern zufolge handelte es sich in Wirklichkeit aber um einen Trojaner, der Android-Smartphones mit der Spyware SMSVova infizierte. Auf bis zu fünf Millionen beläuft sich Schätzungen zufolge die Zahl der App-Downloads. Der Code der App enthielt offenbar auch Bestandteile des Trojaners DroidJack, der 2015 als besonders perfides Werkzeug zur Ausforschung von Smartphone-Nutzern in die Schlagzeilen geriet. DroidJack ist unter anderem in der Lage, den Datenverkehr zu überwachen, Telefon- und Umgebungsgespräche abzuhören sowie Aufnahmen mit der Smartphone-Kamera unbemerkt auszulösen.

Dialer

Dialern sind Programme, die Telefonverbindungen (zur Verbindung mit dem Internet) unterbrechen und Verbindungen zu teuren Sonderrufnummern aufbauen. Diese Programme verursachen schwerwiegende Probleme und lassen Ihre Rechnung bedeutend ansteigen.

Kann ich von Dialer-Programmen infiziert werden?

Kabel User haben mit Dialern kein Problem, da diese Verbindung nicht ohne weiteres verändert werden kann daher gibt es hier feste Zugangsdaten und keine frei wählbare Einwählverbindung. Anders sieht es bei Modem- oder ISDN-Nutzern aus, hier kann ein Dialer die Einwählnummer so verändern, dass eine kostenpflichtige Telefonnummer (0900, 0901 und 0906) benutzt wird.

Was kann ich als Modem- oder ISDN-Nutzer gegen Dialer tun?

Der beste Schutz gegen Missbräuche ist, zu verhindern, dass solche Nummern von Ihrem Gerät aus eingestellt werden können. Jeder Anbieter in der Schweiz ist dazu verpflichtet, seinen Kundinnen und Kunden ein Möglichkeit zu geben, nur die 0906- oder alle 090x- Nummern zu sperren. Die Sperrung muss durch die Teilnehmerinnen und Teilnehmer einfach und gratis

aktiviert und deaktiviert werden können. Ihr Anbieter muss Sie über die Sperrmöglichkeiten beim Abschluss eines neuen Vertrages und danach mindestens einmal jährlich informieren. Zusatzlich muss der Zugang zu Erotikdiensten (0906) für alle Benutzer unter 16 Jahren von vorneherein so weit wie möglich gesperrt werden.

Dialer auf der Festplatte, was kann ich tun?

Natürlich kann es trotz aller Sicherheitsmassnahmen vorkommen, dass ein Dialer den Weg auf Ihrem Computer findet. Wichtig ist hierbei, dass Sie den Dialern nicht sofort löschen oder gar die Festplatte formatieren. Sie brauchen nämlich die Dialerndaten als Beweismaterial, damit Sie nachweisen können, dass Sie diese Telefonnummer nicht freiwillig eingerichtet haben. Dieser Nachweis ist für Ihr Telekommunikationsunternehmen wichtig, denn damit können Sie die zahlung von Dialertelefonrechnungen verweigern. Ohne den Dialer auf Ihrer Festplatte, können Sie einen solchen nachweis nicht führen. Am besten bringen Sie Ihr infiziertes Gerät zu einem Fachmann für Computersicherheit, der Ihnen bestätigen kann, dass sich ein solcher Dialer ungefragt auf Ihrem System installiert hat. Zudem kann man unter folgender Website den Inhaber der fraglichen Nummer suchen.

Bestimmen Sie welche Telefonnummer zu einem Dialer gehört:

- ❏ 1. +41 78 906 7005
- ❏ 2. 0906 333333
- ❏ 3. 001-212-324-4152
- ❏ 4. 0900 123456
- ❏ 5. 0901 234567
- ❏ 6. 058 399 3209
- ❏ 7. 044 446 96 00

Korrekte Antworten:
2. / 4. / 5.

Spam-Mails

Unter Spam (oft auch als Junk bezeichnet) versteht man den nicht angeforderten und unerwünschten Versand von Nachrichten über den elektronischen Weg. Diese Nachrichten werden meist an zahlreiche Empfänger verschickt (oftmals per Mail) und füllen unablässig die digitalen Postfächer dieser Welt. Den Hauptteil bilden hierbei ungebetene Massen-Mails (UBE – unsolicited bulk e-mail) wie beispielsweise Kettenbriefe und unerwünschte kommerzielle Mails (UCE – unsolicited commercial e-mail). Durch solche Mails sollen die Empfänger in der Regel angeregt werden, ein bestimmtes Produkt zu kaufen, persönlichen Daten weiterzugeben, einen Link zu einer Website anklicken oder einen Dateianhang zu öffnen. Spam-E-Mails machen momentan ca. die Hälfte aller verschickten E-Mails weltweit aus.

Verschiedene Arten von Spam-Mails

Spam tritt zwar nicht nur im Mail-Verkehr auf, wird aber vorwiegend durch diesen verbreitet. Die Urheber werden als Spammer bezeichnet. Die meisten nutzen spezielle Computerprogramme, die Spambot oder E-Mail-Harvester genannt werden. Viele Junk-Mails beinhalten Werbung für (oftmals dubiose) Produkte, Falschmeldungen, Links zu Phishing-Websites oder Schadprogramme.

Die gängigsten Formen von Spam-Mails lassen sich den folgenden vier Gruppen zuordnen:

- **Werbung:** Anbieter von billigen Armbanduhren (welche bekannte Luxus-Modelle nachahmen), nichtlizensierte Medikamenten (häufig Viagra) oder illegalen Internetinhalten nutzen häufig Spam zum Anpreisen ihrer Produkte. Zu den typischen Inhalten der werbenden Spam-Mails gehören auch Links zu angeblich kostenlosen Angeboten, die dann

in Abofallen führen, oder Verweise auf angeblich reichmachende Geschäftsmodelle. Letztere müssen dann kostenpflichtig heruntergeladen werden und machen lediglich den Spammer reich.

- **Falschmeldungen:** In vielen Spam-Mails befinden sich Aufrufe, Warnhinweise oder Geschichten, die wenig vertrauensvoll erscheinen. Im Englischen werden sie als Hoax (Scherz/Falschmeldung) bezeichnet. Die Inhalte solcher Mails sind oft frei erfunden oder tatsachenfremd und effekthascherisch zugespitzt. Wenn sie von den Empfängern für voll genommen und weitergeleitet werden, kann sich solch eine Falschmeldung über das Schneeball-Prinzip rasant verbreiten.
- **Phishing:** In dieser Form von Spam wird vorgegeben, dass der Absender der Nachricht zu einem bestimmten Unternehmen (meist einer Bank) gehört. Der Empfänger wird aufgefordert persönliche Daten wie Konto- und Kreditkartendetails mit den dazugehörigen Passwörtern anzugeben. Zu diesem Zweck haben die Phishing-Betrüger oft Websites erstellt, auf denen in den Spam-Mails verlinkt wird und die denen offizieller Banken täuschend ähnlich sehen. Wenn man dort seine privaten Daten angibt, gelangen selbige in die Hände von Cyberkriminellen.
- **Schadprogramme**: Über Spam-Mails gelangen häufig Schadprogramme (auch Malware, Evilware oder Junkware genannt) auf einen Rechner. Hierzu zählen beispielsweise Computerviren und -würmer, Trojaner oder Spyware. Durch das Öffnen von Programmen, Links oder Mailanhängen dringen sie ins System ein. Von dort lassen sie sich meist nur noch durch Antivirenprogramme oder andere spezielle Software entfernen.

So können Sie sich gegen Spam- oder Phishing Mails schützen

Früher konnte man ein Spam- oder Phishing Mail an den vielen Grammatikfehlern erkennen. Das ist heute kaum mehr so. Im Gegenteil: Die Absender benutzen namen bekannter Unternehmen und kopieren auch deren E-Mail Layouts. Mit folgenden Tipps schützen Sie sich vermehrt vor Spam.

Mehrere E-Mail Adressen

Damit weniger Spam- und Phishing E-mails in Ihrem E-Mail Postfach landen, sollten Sie mindestens zwei verschiedene E-Mail-Adressen nutzen. Eine Adresse, die Sie nur an Bekannte weitergeben und eine weitere für Gewinnspiele, Foren und Online-Einkäufe. Für einmalige

Dineste wie zum Beispiel eine Teilnahme an einer Umfrage, können Sie auch eine Wegwerf-Adresse (z.B.10minutemail.com) nutzen.

Spam an den Provider melden

Grosse Anbieter wie z.B. Gmail filtern ihre E-Mails auf Spam. Dabei werden alle eingehenden und ausgehenden E-mails systematisch auf spam-typische Elemente überprüft. Weist ein E-Mail verdächtige merkmale auf, gelangt es automatisch in den Spam-ordner. Wenn sie trotzdem Spam-E-Mails erhalten, sollten sie diese als Spam kennzeichnen (Tutorial).

Überprüfen Sie ihre Mails vor dem Öffnen

Damit Sie nicht in die Spam-Falle tappen, sollen Sie jedes E-Mail rasch prüfen, bevor Sie es öffnen:

- Ist der Absendername und die Absender E-Mail Adresse bekannt?
- Ist der Betreff sinnvoll?
- Wird ein Anhang von diesem Absender erwartet?

Ergeben diese drei Punkte kein stimmiges Bild, markieren sie das E-Mail als Spam und löschen es danach. So schützen Sie sich, aber auch andere Nutzer. Denn wenn viele Empfänger ein E-Mail als Spam markieren, landet es künftig bei allen direkt im Spam-Ordner. Wichtig ist, dass Sie niemals ein Link oder Anhang in einer Spam-verdächtigen E-Mail öffnen. So kann Ihnen, Ihren Daten und Ihrem Computer nichts passieren.

Bestimmen Sie welche Mails Spam-verdächtig sind:

1. Microsoft Account

From: "Microsoft Team" <inegon06@netscape.com>
Date: 7 October 2015 at 17:53:10 BST
To: <customerservice@outlook.com>
Subject: Avoid Suspension 2015!!!

Outlook

Dear Subscriber,

Your Microsoft account has been compromised.You must update it immediately or your account will be closed.

Click here to update

Sincerely,

Microsoft Online Security Team

2. Information an Kursteilnehmer

üK Klassen Posteingang ×

ZLI - Svenja Schnyder <svenja.schnyder@zli.ch>
an svenja.schnyder

Sehr geehrte ÜK Teilnehmenden

Gemäss Bundesratsentscheid bleiben bis am 4. April 2020 schweizweit alle Schulen geschlossen. Daher müssen auch wir den Unterricht pausieren.

Jede Klasse erhält anfangs nächste Woche separat weitere Informationen wie wir mit dem Unterricht in einer anderen Form weiterfahren oder Umplanen.

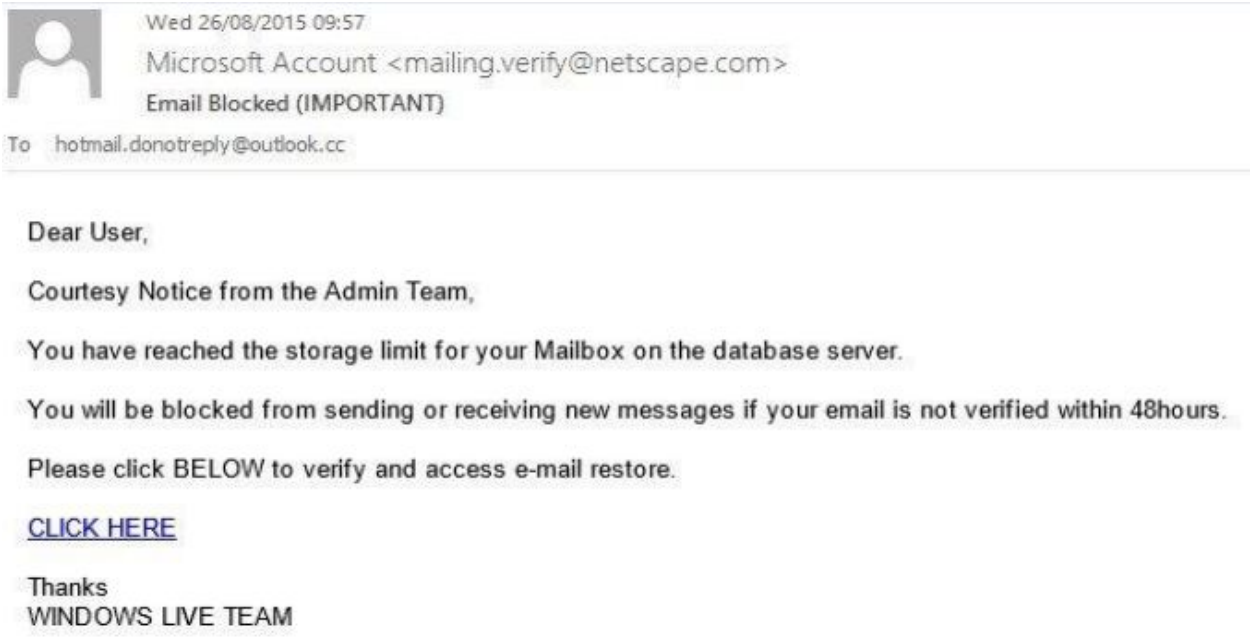
Ihre Berufsbildner erhalten dieses Mail zur Kenntnisnahme.

Wir wünschen Ihnen trotz der ausserordentlichen Situation ein schönes Wochenende.

Freundliche Grüsse
Svenja Schnyder
Sachbearbeiterin

--
Zürcher Lehrbetriebsverband ICT
Edenstrasse 20, 8045 Zürich
T 044 552 8200
https://www.zli.ch

3. Mailbox voll



Wed 26/08/2015 09:57

Microsoft Account <mailing.verify@netscape.com>

Email Blocked (IMPORTANT)

To hotmail.donotreply@outlook.cc

Dear User,

Courtesy Notice from the Admin Team,

You have reached the storage limit for your Mailbox on the database server.

You will be blocked from sending or receiving new messages if your email is not verified within 48hours.

Please click BELOW to verify and access e-mail restore.

CLICK HERE

Thanks
WINDOWS LIVE TEAM

Korrekte Antworten:

1. Dies ist ein Spam-Email. Das Mail kommt nicht aus einer von Microsoft offiziellen genutzten Domain. Zudem muss ein Account nie aktualisiert werden, ohne eine direkte Begründung. Aufforderungen wie “Click here” sind nicht sehr vertrauenswürdig. Zudem haben Mails von Firmen wie Microsoft meistens HTML Elemente, sprich sie sehen aus wie eine Website.

2. Dies ist ein normales Mail. Die Domain kommt aus dem selben Haus wie der Kursveranstalter (ZLI). Der Text macht Sinn und das Mail wird durch eine standardisierte Signatur beendet, ein Wiedererkennungsmerkmal für deren E-Mails.

3. Dies ist ein Spam-Email. Das Mail kommt nicht aus einer von Microsoft offiziellen genutzten Domain. Seriöse Mails werden niemals im Capslock irgendwelche Aufforderungen machen einen link zu öffnen. Die Signatur wirkt ebenfalls kaum seriös. Zudem ist das Mail an niemand explizit gerichtet sondern ist eine allgemeine Begrüssung. Firmen wie Microsoft verwenden personalisierte Begrüssungen.