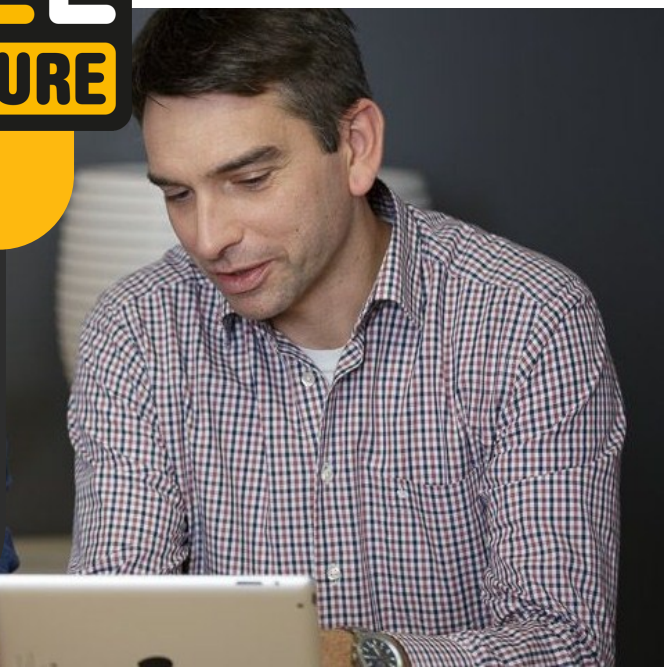
Den Computer schützen:
Warum eigentlich?



INHALT

Ein Virus legt Ihren Computer lahm – er ist vorübergehend nicht zu benutzen und muss repariert werden. Wie ärgerlich! Wenn Sie, wie die meisten Internetbenutzer, glauben, dieser kurzzeitige Verlust an Verfügbarkeit sei das Schlimmste, was Ihnen passieren kann, ist Ihnen wohl nicht bewusst, dass dies nur die Spitze des Eisbergs ist! Das eigentliche Ausmaß eines IT-Angriffs offenbart sich selten. Denn Cyberkriminelle finden auf nahezu jedem Arbeitscomputer „Beute“ von hohem Wert. Beute, die Sie als rechtmäßiger Besitzer vielleicht gar nicht als solche wahrnehmen, deren Abhandenkommen jedoch einen enormen Schaden anrichten kann.
Dazu gehören:

1. BENUTZERNAMEN UND PASSWÖRTER

An Benutzernamen und Passwörter gelangen Cyberkriminelle etwa mithilfe von Phishing-Mails oder Trojanern, die alle Ihre Tastatur-Eingaben mitschreiben.

Oft ist sogar das nicht einmal notwendig: Benutzen Sie ein simples Passwort, ist es mithilfe des richtigen Programms oder eines Social Engineers binnen Sekunden „erraten“.
Login-Daten sind wertvoll für die Piraten, denn sie erlauben es, sich in Ihrem Namen bei Online-Diensten einzuloggen.
Zum Beispiel:

- Bei Servern Ihrer Firma, um an firmeninterne Daten zu gelangen
- Bei Ihrer Bank, um Geld von Ihrem Konto zu stehlen
- Bei Ihrem Online-Server, um auf dort gespeicherte Dateien zurückzugreifen
- Bei Ihrem Online-Shopping-Portal, um Waren in Ihrem Namen und auf Ihre Rechnung zu kaufen
- Bei Ihrem sozialen Netzwerk, Ihrem E-Mail-Account oder Chat-Zugang, um Ihre Online-Identität zu übernehmen und damit Betrug zu begehen

2. PERSÖNLICHE KONTAKTE

Cyberkriminelle sammeln Namen, E-Mail-Adressen und Telefonnummern von Leuten aus Ihrer Kontaktliste, um sie an Dritte weiterzuverkaufen. Diese benutzen sie dann wiederum, um Spam oder Phishing-Mails zu verschicken, mit denen die kriminellen Maschen dann weitere Kreise ziehen.

Wenn Sie Kontakt zu Personen des öffentlichen Lebens oder in leitenden Positionen gewisser Industrien haben, könnten Kriminelle auch gezielt nach deren Kontaktinformationen fahnden.

3. SENSIBLE KOMMUNIKATIONEN

Führen Sie wichtige private oder berufliche Diskussionen per E-Mail und Messenger? Auch Kriminelle könnten an den Inhalten interessiert sein.

Seien Sie sich bewusst, dass sich E-Mail als Kommunikationsmittel nicht zum Versenden von vertraulichen und schon gar nicht von geheimen Daten eignet.

4. VIRTUELLE GÜTER

Cyberkriminelle werfen ein Auge auf alles, was sie zu Geld machen können. Dazu gehören auch nicht-materielle Güter wie Computerspiel-Charaktere, -Items oder –Zahlungsmittel und hohe Spielstände, die sich leicht kopieren und dann weiterverkaufen lassen. Genauso lukrativ sind Ihre Softwarelizenzen, Betriebssystem-Lizenzschlüssel oder Spiellizenzen.

5. ÜBERSICHT IHRER FINANZSITUATION

Haben Cyberkriminelle Zugriff auf Ihren Computer, können sie ihn nach wertvollen Informationen durchsuchen. Zum Beispiel nach Kreditkarteninformationen, Steuerdaten oder Investmentplänen. Solche Auskunft über Ihre finanzielle Situation kann entscheidend dafür sein, ob und inwiefern Sie weiterhin im Visier der Kriminellen bleiben.

6. IHR COMPUTER ALS TEIL EINES GROßEN NETZWERKS

Bot-Netze sind große Netzwerke von kompromittierten Computern (auch „Zombies“ genannt), die von außen kontrolliert und ferngesteuert werden.

Ohne dass Sie es merken, kann Ihr Computer Teil eines solchen Netzes werden und kann dann für kriminelle Aktivitäten missbraucht werden, wie etwa das Versenden von SPAM und Phishing-Mails an Millionen von Benutzern weltweit, oder zum Durchführen von Denial of Service Attacken, die ganze Webseiten und Webdienste lahmlegen. Die Quelle des Übels ist Ihr Computer, auch wenn Sie persönlich nicht aktiv waren.

7. IHR COMPUTER ALS WEBSERVER

Ebenfalls gefährlich: Kriminelle können Ihren Computer in einen Webserver verwandeln, den sie dann für die Bereitstellung illegaler Inhalte benutzen. Zu diesen Inhalten gehören:

- Phishing-Webseiten, die dazu dienen, Login- oder Bankdaten ahnungsloser Benutzer zu stehlen
- Angriffswerkzeuge, mit denen die Computer ahnungsloser Dritter kompromittiert werden können
- Kinderpornografisches Material, Raubkopien von Videos und Musik

8. IHR COMPUTER ALS MITTEL ZUR ERPRESSUNG

Eine sehr gängige Methode von Cyberkriminellen besteht darin, den Computer ihres Opfers mit Schadprogrammen zu infizieren, und dann Geld zu verlangen, um ihn wieder zu „säubern“.
Oder aber es werden alle auf dem Computer befindlichen Daten nach einem Schema verschlüsselt, das nur den Kriminellen bekannt ist. In diesem Fall wird eine beträchtliche Geldsumme für die Entschlüsselung gefordert.
Zahlen Sie nicht, drohen die Kriminellen damit, sämtliche Daten zu zerstören.

Haben Sie problematische Inhalte, wie z.B. Pornografie, im Web konsumiert, einen intimen Web-Cam-Chat betrieben oder etwa in Netzwerken und Foren unter einem Pseudonym sensible Aussagen gemacht, könnte es sein, dass Kriminelle darüber Protokoll geführt haben und für die Nicht-Veröffentlichung Geld verlangen.

Besonders wenn Sie eine Person des öffentlichen Lebens sind, sollten Sie sich vor dieser Art von Interventionen in Acht nehmen.

9. WIE SIE ERKENNEN, OB IHR COMPUTER GEHACKT WURDE

Ist ein Schadprogramm gut geschrieben, ist es schwer bis unmöglich, die Infektion des Computers als Laie festzustellen. Achten Sie dennoch auf Anomalien:

- Läuft Ihr Computer viel langsamer als sonst?
- Schlägt Ihr Antivirenprogramm Alarm?
- Werden Sie bei einer Suche auf Google plötzlich auf Resultate in anderen Suchmaschinen geleitet?
- Sprechen Freunde Sie darauf an, eigenartige E-Mails oder Nachrichten von Ihnen erhalten zu haben?
- Wurde Ihr E-Mail-Konto oder Ihr Profil im sozialen Netzwerk gesperrt, etwa weil Spam darüber verteilt wurde?
- Schaltet sich Ihre Webcam von selbst an?
- Taucht, unabhängig von den besuchten Webseiten, Werbung in Ihrem Betriebssystem auf?
- Stürzt Ihr Computer während eines Software-Updates unerwartet ab?

Dies sind nur einige von vielen möglichen Anzeichen dafür, dass Ihr Computer infiziert ist.

Wenn Sie die Möglichkeit haben, benutzen Sie eine Live-CD*, um das Gerät zu scannen. Dieser Vorgang ermöglicht eine Analyse des Computers, ohne das Hauptsystem zu starten und eignet sich deshalb sehr gut für Antiviren-Operationen.
Ebenfalls ratsam: ein Backup Ihrer Daten durchführen, und den Computer anschließend neu installieren. Falls Sie sich von diesen Maßnahmen überfordert fühlen, wenden Sie sich an einen IT-Sicherheitsexperten, z.B. an einen „PC Doctor“*.

Wie immer gilt die Devise: Vorsicht ist besser als Nachsicht! Um die Verwundbarkeit Ihres Computers so gering wie möglich zu halten, sollten Sie präventiv technische Schutzmaßnahmen anwenden und auf ein sicheres Verhalten im Internet achten.

Weitere Informationen unter www.bee-secure.lu