Computacenter

SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT – UMGANG MIT INFORMATIONEN

Malware-Schutz

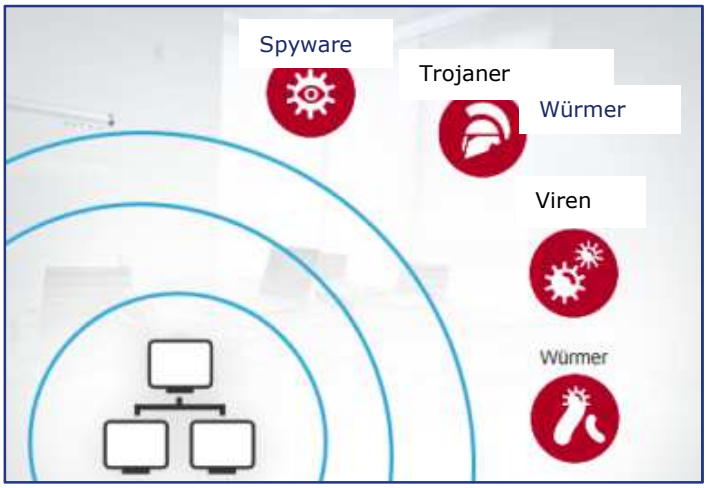
MALWARE-SCHUTZ

Einführung

„Malware-Schutz“

In diesem Abschnitt erfährst Du, welches Risiko für unser IT-Netzwerk von Schadsoftware (engl. **Mal**icious Soft**ware**, kurz Malware) ausgeht und welche technischen Maßnahmen wir zu unserem Schutz eingeführt haben.

Angriffe auf unternehmenseigene Datennetzwerke können wegen des enormen Werts, den digitale Informationen darstellen, erheblichen Schaden anrichten.



Malware wird eingesetzt, um von außen in Unternehmensnetzwerke einzudringen und die dort vorhandenen Daten zu manipulieren bzw. zu entwenden. Zur Kategorie der Malware gehören beispielsweise Würmer, Trojaner und Spyware.

Die am häufigsten genutzten Methoden, um Computer mit Malware zu infizieren, lassen sich eigentlich ganz einfach verhindern:

Denke noch einmal nach… bevor du auf einen Link klickst

Dabei handelt es sich um Links in unseriösen E-Mails oder Links auf Websites, die Dich dazu bringen sollen, auf sie zu klicken. Weit verbreitet ist die Behauptung, Du hättest einen Preis gewonnen oder eine Rechnung noch nicht beglichen.

Denke noch einmal nach… bevor du verdächtig aussehende E-Mails oder deren Anhänge öffnest

Diese werden manchmal über seriös wirkende E-Mail-Adressen verschickt. Der Betreff der E-Mail kann jedoch verdächtig erscheinen, oder die tatsächliche Adresse des Absenders unterscheidet sich von der, die angezeigt wird.

©Computacenter (UK) Ltd 2019

Viren

Viren sind lokale Schadprogramme, d. h. sie können sich auf dem infizierten Computer verbreiten. Auf andere Computern gelangen sie, wenn ein Nutzer infizierte Dateien weitergibt.

Viren kann man sich unter anderem beim Herunterladen oder Surfen im Internet einfangen. Sie können Datenverluste verursachen, Daten an unberechtigte Dritte weiterleiten oder die Funktionsfähigkeit des Computers beeinträchtigen.

Würmer

Würmer können sich selbständig per Netzwerk- oder Internetverbindung von einem Computer auf den anderen verbreiten. Sie können völlig harmlos aussehen, sind es aber nicht.

Denn Würmer versuchen z. B., eine bestimmte Webseite aufzurufen. Geschieht dies zeitgleich von vielen infizierten Rechnern aus, wird diese Seite lahmgelegt: eine so genannte„Denial-of-Service“-Attacke. Werden über die betroffene Seite Geschäfte abgewickelt, kann so ein großer Schaden entstehen.

Trojaner

Trojaner tarnen sich oft als nützliche Hilfsprogramme. Sie werden in der Regel vom Anwender auf den PC geladen, z. B. über infizierte Software.

Diese Schadprogramme können dann beispielsweise Passwörter ausspionieren und unerkannt an einen Dritten weiterleiten – oder ermöglichen es diesem sogar, Ihren Rechner komplett fernzusteuern. Haben Sie sich einen Trojaner eingefangen, können Sie keiner Bildschirmanzeige mehr vertrauen.

Spyware

Spyware-Programme sammeln Daten und leiten sie an Dritte weiter, z. B. um …

- gültige E-Mail-Adressen zu sammeln.
- Nutzerprofile zu erstellen.(Welche Programme verwenden Sie? Welche Webseiten besuchen Sie?)
- anhand von Geodaten (etwa eines Smartphones) Bewegungsprofile zu erstellen.

Antiviren

Ein Antivirenprogramm schützt das Unternehmensnetzwerk – nicht nur gegen Viren, sondern auch gegen viele andere Arten von Malware. Technische Verfahren dienen dazu, Malware automatisch zu erkennen und zu melden und nach Möglichkeit zu entfernen und auszuschalten.

Antivirenprogramme müssen laufend aktualisiert werden, damit sie Malware verlässlich erkennen können.

©Computacenter (UK) Ltd 2019

Wenn Du regelmäßig außerhalb des Büros unterwegs bist, solltest Du Dich mindestens einmal pro Woche (per VPN) beim Computacenter-Netzwerk anmelden. Hierdurch werden die Software-Updates automatisch auf Deinem Gerät installiert.

Szenarien

Eine der einfachsten Wege, wie Malware in ein Netzwerk gelangen kann, ist die achtlose Nutzung eines USB-Sticks oder eines anderen Wechseldatenträgers.

So vermeidest Du eine Malware-Infektion:

- Es sollten ausschließlich unternehmenseigene Wechseldatenträger verwendet werden.
- Sämtliche Datenträger müssen vor der Verwendung auf Viren gescannt werden.
- Wird ein USB-Gerät zur Datenübertragung eingesetzt, sollte es ebenfalls zunächst formatiert und dann auf Viren gescannt werden.
- Nach der Übertragung können die Daten dann von dem Gerät gelöscht und das Gerät selbst neu formatiert werden.

Zusammenfassung

In diesem Abschnitt hast Du gelernt...

- dass das Unternehmensnetzwerk durch Malware (Viren, Würmer, Trojaner, Spyware) erheblichen Risiken ausgesetzt ist.
- dass Du noch einmal nachdenken solltest, bevor Du auf Anhänge und Links klickst
- dass zum Schutz unserer IT-Infrastruktur sämtliche Wechseldatenträger vor ihrer Verwendung auf Viren gescannt werden sollten.

<u>Datenschutzverletzungen und Informationssicherheitsvorfälle:</u>

Wenn Du glaubst, dass Deine Geräte mit Malware infiziert wurden, melde bitte einen entsprechenden Informationssicherheitsvorfall über das NGSD.

©Computacenter (UK) Ltd 2019