INFO

Viren und Trojaner auf dem Vormarsch: Wie Sie Ihr System wirkungsvoll schützen können!

Schadsoftware

Entwickler von Computerviren sind sehr kreativ und ihren Gegnern immer einen Schritt voraus. Doch der Angreifer hat eine Schwachstelle: ***er braucht Partner****. Bedauerlicherweise* ***verbünden wir selbst (!) uns mit diesen Angreifern*** *und werden natürlich sofort zu ihren Opfern. Paradox? Ja, und leider allzu menschlich.*

Aktuell haben wir es wiederholt mit einer wahren Welle an Viren und Trojanern zu tun.
Mittlerweile geht die Bedrohung nicht mehr nur von E-Mails aus, auch andere Medien werden genutzt um Schädlinge einzuschleusen.
Als aktuelle Bedrohung 05/2017 ist die Ransomware mit dem Namen **WannaCry (**bzw. schon Weiterentwicklungen unter anderen Namen) zu nennen, welche momentan aggressiv verbreitet werden.
Dabei kann man mit etwas Aufmerksamkeit und der Befolgung weniger Regeln die meisten Angriffe abwehren.

Aktuelle Bedrohungslage

Aktuelle Beispiele:

Beispiel: Angriff über eine Windows-Sicherheitslücke (SMB):

- Der Virus **WannaCry** verbreitet sich über eine bekannt gewordene Sicherheitslücke im Windows-System (SMB)
- Einmal im Netzwerk, verbreitet sich der Virus wie ein Wurm und infiziert weitere Computer/Server
- Die befallenen Systeme werden verschlüsselt und erhalten einen kryptischen Namen

INFO: Da dieser Virus nicht zwingend eine Interaktion des Users voraussetzt, sondern direkt auf die Sicherheitslücke im System zielt, sollten dringend und umgehend alle aktuellen Patches von Microsoft installiert werden.

Gerne steht Ihnen CVS zur Aktualisierung ihrer Systeme zur Verfügung und vereinbart kurzfristig einen Termin mit Ihnen!

Umgang mit E-Mails

Immer folgende Fragen stellen:

- Erwarte ich eine Mail von diesem Absender?
- Stammt die Mail wirklich vom angegebenen Absender?

- Enthält die Mail Links oder Anhänge?
- Werde ich aufgefordert, Links anzuklicken und Anhänge zu öffnen?

Können diese Fragen nicht eindeutig beantworten werden, sollte man diese Mail nicht öffnen bzw. direkt löschen.
Sollten Sie dennoch unsicher sein, stehen wir Ihnen natürlich gerne beratend zur Seite.

Vorsicht Falle im Umgang mit E-Mails!

Den Absender zu kennen, bedeutet aber noch keine vollständige Sicherheit. Begegnen Sie besser jedem Anhang mit Vorsicht. „Seriöse“ E-Mail-Accounts können **gekapert** und zur Versendung von Schadsoftware genutzt werden! Im Verdachtsfall ist eine kurze Antwort-Mail mit der Bitte um eine Erklärung der einfachste Weg.

Betrachten Sie auch **Links zu externen Web-Seiten** grundsätzlich kritisch. Wenn Ihnen Ihr Steuerberater plötzlich einen Link zu niedlichen Katzenfilmchen schickt, sollten Sie Verdacht schöpfen. Doch auch ein plausibler Link sollte vor dem Anklicken kurz überprüft werden – siehe Kasten.

Fazit: Das bisher Beschriebene richtet sich an uns als Anwender, die manchmal etwas unbedarft mit E-Mails umgehen. Denken Sie auch an Mitarbeiter bzw. Kollegen, die eher selten mit dem Medium E-Mail zu tun haben, und klären Sie diese entsprechend auf!

Datensicherung

Menschen machen Fehler. Sicherheitssysteme können sie vielleicht verhindern, mindestens aber deren Folgen begrenzen. **Ohne eine funktionierende Datensicherung riskieren Sie Ihr Unternehmen!**

Sie sichern Ihre Daten regelmäßig? Gut! Aber ein erfolgter Sicherungslauf ist nicht zwingend ein erfolgreicher. Verschickt Ihr Datensicherungssystem schon eine **E-Mail** mit dem **Status des erfolgten Sicherungslaufs** – ggf. mit einer Info über entstandene Probleme? Besser wäre es! Wir richten es Ihnen gern ein. Eine Problemmeldung können Sie an unsere Techniker weiterleiten, die sich um alles Weitere kümmern. So haben Sie einen der wichtigsten Parameter für den Bestand Ihres Unternehmens immer auf dem „Radarschirm“.

Verschlüsselungstrojaner

Aktuell sehr verbreitete Angriffe sind zweistufig organisiert: **1. Verschlüsselung** Ihrer gesamten Daten, **2. Erpressung** von „Lösegeld“ für die Dechiffrierung. Währung: Bitcoins. Zahlen Sie nicht, sind Ihre Daten verloren.

War ein solcher Abgriff erfolgreich (weil das „Partnermodell“ – siehe oben – funktioniert hat), wird es teuer: Ihr Netzwerk ist für die Dauer der „Entseuchung“ und der Rücksicherung „sauberer“ Daten lahmgelegt. Ob die überhaupt verfügbar sind, hängt von Ihrer Datensicherung ab. Welche Sicherungsstände gibt es? Wie oft sichern Sie?

Doch auch ein ausreichender Bestand an Sicherungsdaten garantiert keine Problemfreiheit. Manche **Schadsoftware wirkt verzögert** und entfaltet erst spät ihre destruktive Gesamtwirkung. Davor macht sie sich allenfalls durch **kleine Auffälligkeiten** bemerkbar. **Bleiben diese über mehrere Tage unbeachtet, werden bereits verseuchte Tagesdaten gesichert**. Im schlimmsten Fall ist der gesamte Sicherungsbestand betroffen.

Deshalb: Stellen Sie etwas **Ungewöhnliches** bei Ihrem PC oder in Ihrem Netzwerk fest, beispielsweise eine plötzlich nicht mehr funktionierende Anwendung, **fahren Sie Ihren Rechner**

sofort herunter, und verständigen Sie umgehend Ihren Systemverwalter. Wir sind selbstverständlich gern behilflich.

Zu guter Letzt …

Angriffe mit Viren und Trojanern sind nichts Neues, aber die Qualität der Methoden und der Schadsoftware hat sich im Sinne der Angreifer deutlich verbessert. Auch sind längst nicht mehr nur Konzerne Ziele der Angreifer. Lukrativ sind ebenfalls kleinere und mittlere Unternehmen – da bringt die Menge den Profit. Die Einstiegsschwelle in den cyber-kriminellen „Markt“ ist niedrig, das Entdeckungsrisiko gering. Wo früher Hacker-Expertise nötig war, können heute regelrechte Baukästen für solche Angriffe gekauft und kann das Erpressungsgeschäft im Nebenerwerb betrieben werden. Und das ist so gefährlich wie banal. Vergleichbar banal sind aber auch die oben beschriebenen Schutzmechanismen – und überdies wirkungsvoll. Selbstverständlich müssen die technischen Schutzeinrichtungen für Ihre Netzwerke auf dem neuesten Stand sein. Auch in dieser Frage beraten wir Sie gern.

Ihr CVS-Team