Malware-Infektionswege: Schadsoftware abwehren

Wie sich Unternehmen schützen können

Seit Jahren nimmt die Verbreitung von Malware zu, und täglich kommen neue Arten von Viren, Würmern und Trojanern hinzu. Bedingt durch das immer bessere Sicherheitsbewusstsein der Benutzer und bessere Erkennungsraten von Antivirensoftware ändert Malware ständig die Infektionswege. Allerdings dauert es im Schnitt 18 Tage vom Auftreten einer neuen Bedrohung (Zero-Day) bis zur Entwicklung und Installation des „Gegenmittels" durch die Virenschutz-Industrie. In dieser Zeitspanne ist jedes System trotz aktueller Software verwundbar.

- E-Mails: Inzwischen sind sich die meisten Benutzer der Gefahren bewusst, die in E-Mail-Anhängen lauern können. Ausführbare Dateien werden häufig schon durch Provider herausgefiltert und viele Anwender wissen bereits, dass man ‚fremde' Dateien nicht mehr sorglos starten soll – besonders bei unbekannten Anwendungen. Daher missbraucht Malware zunehmend bekannte und oftmals unverdächtig erscheinende Formate, wie beispielsweise PDF oder Office-Dateien (z.B. Makros in Excel) als Einfallstor.
- Direkte Downloads: Downloadplattformen aller Art, aber gerade auch Gratis-Filme oder Musik sind immer noch die häufigsten Methode, wie man sich gefährliche Dateien auf den Rechner holt. Wenn Mitarbeiter am Firmensystem auf Pirate Bay oder ähnlichen Plattformen regen Austausch betreiben, ist höchste Alarmbereitschaft angesagt!
- Drive-by-Infektionen: Neben der klassischen Infektion über Dateien werden immer mehr sogenannte Drive-by-Infektionen beobachtet. Dabei wird der Rechner unbemerkt im Hintergrund infiziert, zum Beispiel beim Surfen auf einer sonst harmlosen Webseite. Als Einfallstor dienen hier der Web Browser und seine zahlreichen Plugins – allen voran Flash, Java oder Silverlight. Dabei ist die Seite, die geladen wird, meist gar nicht der Verursacher, sondern selbst das Opfer von Cyberkriminellen.

Wie kann ich mich schützen?

- Auf allen Geräten Virenscanner und Firewall nutzen: Es klingt selbstverständlich, aber leider sind noch immer viele Rechner nicht oder unzureichend geschützt. Nähere Infos finden sie auch auf dem Infoblatt Virenschutz & Firewall!
- Regelmäßige Updates: Auch wenn es mitunter nerven kann, sollte man den Programmen stets erlauben, die Aktualisierungen durchzuführen. Das gilt für Betriebssysteme, Browser (auch Plug-Ins & Add-ons) und natürlich ganz besonders für Virenscanner & Firewall. Aktuelle Versionen schließen immer Sicherheitslücken der Vorgänger – Studien zeigen, dass sich über 95 % der Angriffe dadurch verhindern lassen.
- Vorsicht ist besser als Nachsicht: Die abgedroschene Floskel ist in diesem Zusammenhang leider wieder einmal richtig! Ein beachtlicher Teil der Malware-Infektionen ließe sich durch vorsichtigere User vermeiden: Nur über gesicherte Portale herunterladen, keine E-Mail-Anhänge von unbekannten Absendern öffnen – allgemein gesagt: nichts anklicken, das man nicht kennt. Damit schützt man nicht nur sich selbst, sondern verhindert auch, dass man Rechner anderer schadet.

Stand: 18.12.2018