Virenschutz im KMU-Umfeld

Virenschutz gehört zur Grundausstattung eines jeden Unternehmens, denn Malware stellt eine stark wachsende Gefahr in der digitalen Welt dar – insbesondere auch für KMU. Ein konsequent betriebener technischer Virenschutz und bewusstes menschliches Verhalten schaffen hier bestmögliche Abhilfe.

Wichtigste Merkpunkte:

- Definieren und implementieren Sie in Ihrem KMU einen **Virenschutzprozess**.
- Erstellen Sie eine Übersicht über Einfalls- und **Verbreitungswege** von Malware in Ihrem Unternehmen.
- Legen Sie in einem **Virenschutzkonzept** fest, wo im Netzwerk die effizientesten Checkpoints für den Virenschutz aufgestellt werden.
- **Sensibilisieren** Sie die Mitarbeitenden für die Gefahren durch Malware.

Der Virenschutzprozess

Heutzutage bieten zahlreiche Hersteller sehr gute Antiviren-Schutzsysteme an, welche sich an die unterschiedlichsten Bedürfnisse und Gegebenheiten in KMU-Netzwerken anpassen lassen. In einer vorgängigen Analyse muss zunächst jedoch die optimale Lösung evaluiert und anschliessend fachmännisch implementiert werden.

Damit ist die Sache aber nicht erledigt: So wie sich Cyberkriminalität und Malware stetig weiterentwickeln, müssen auch die Schutzmassnahmen dauernd gepflegt und aktualisiert werden. Z. B. muss der Virenschutz stets mit den neusten Virenmustern aufdatiert werden.

Hierfür ist ein Virenschutzprozess zu etablieren, der sowohl die Durchführung der ordnungsgemässen Überwachung der Datenflüsse, und der Erkennung und Beseitigung von Malware (https://www.ebas.ch/malwareinfektion/) , wie auch die Maintenance der Systeme gewährleistet. Ebenso wichtig ist, dass in diesem Prozess regelmässig auch eine Sensibilisierung der Mitarbeitenden für diese Art der Bedrohung erfolgt.

Die Verbreitungswege

In KMU-Netzwerken nimmt die Komplexität stetig zu. Fast täglich werden neue Software-Lösungen implementiert, entstehen neue Datenverbindungen oder wird an der Infrastruktur gefeilt. Cyberkriminelle nutzen die entstehende Komplexität, um immer neue Einfalls- und Verbreitungswege für ihre Malware zu finden und auszunutzen.

Eine möglichst umfassende Identifikation der potenziellen Einfalls- und Verbreitungswege von Malware bildet deshalb die Basis für das Virenschutzkonzept (#concept) . Ein etablierter Ansatz dabei ist das Denken in Szenarien:

1. «Wie und wo könnte ein Angreifer eine Malware in das Netzwerk einschleusen»?
2. «Wie könnte sich die Malware anschliessend im Netzwerk verbreiten»?

Für das Einschleusen von Malware werden häufig insbesondere folgende Kanäle missbraucht:

- Internet-, WLAN- und VPN-Verbindungen

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik

- Anhänge in Kommunikationsmitteln, wie z.B. E-Mail
- Mobilegeräte von Mitarbeitenden und Gästen
- Remote-Desktop- (RDP) und Terminalserver-Anwendungen
- Austausch von physischen Datenträgern
- Ungenügend geschützte IoT-Umgebungen

Einmal im internen Netzwerk angelangt, kann die Malware für die Weiterverbreitung Sicherheitslücken ausnutzen und beispielsweise durch unvorsichtiges Handeln von Mitarbeitenden aktiviert werden und damit ihre schädliche Wirkung entfalten. In solchen Fällen ist es wichtig, den Schaden möglichst begrenzt zu halten und eine grossflächige Verbreitung zu unterbinden.

Das Virenschutzkonzept

Anhand der identifizierten Einfalls- und Verbreitungswege kann nun bestimmt werden, wo im Netzwerk die Virenschutzmassnahmen ihre Wirkung am effizientesten entfalten.

Aufgrund ihrer Exposition sollten dabei insbesondere die ein- und ausgehenden Netzwerkverbindungen zum Internet auf Malware durchleuchtet werden. Dies kann auf der Firewall oder auf Proxy- und Kommunikationsservern erfolgen. Hierbei gilt es zu beachten, dass die Inhalte jeweils vor der Verschlüsselung resp. nach der Entschlüsselung geprüft werden müssen.

Auch mobile Geräte von Mitarbeitenden und Gästen stellen diesbezüglich eine grosse Gefahr dar, weil sie oft auch in ungesicherten Umgebungen betrieben werden. Sie sollten daher nie ungeprüft ins interne Netzwerk gelangen. Dies gilt insbesondere auch für VPN-Verbindungen von extern, z. B. bei Arbeiten im Home-Office (https://www.ebas.ch/5-empfehlungen-fuer-kmu-mit-homeoffice/) . Hier bietet sich eine zentral verwaltete Antiviren-Software auf den Endgeräten an.

Schliesslich müssen auch stationäre Geräte, an denen jedoch externe Datenträger angeschlossen werden, mit einem entsprechenden Virenschutz ausgestattet sein.

Im Virenschutzkonzept werden das gesamte Virenschutzsystem und dessen Konfiguration festgehalten.

Antivirus-Suiten für Unternehmen

Zahlreiche Hersteller bieten Antivirus-Lösungen an, die auch für grössere Netzwerke geeignet sind. Roll-out, Konfiguration und Maintenance des AV-Schutzes kann damit plattform- und standortübergreifend von zentraler Stelle verwaltet werden. Auf diese Weise kann sichergestellt werden, dass die Sicherheitspolicy des KMU eingehalten werden kann, sobald sich ein Gerät mit dem Netzwerk verbindet.

Statistiken zu Cyberkriminalität sprechen eine deutliche Sprache: Malware-Attacken mit Schadenfolge haben in den letzten Jahren signifikant zugenommen. Insbesondere Ransomware stellt für KMU eine ernst zu nehmende Gefahr dar.

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik