Cybercrime und Business

Das Webinar »NextGen Security« von Bechtle gab einen Überblick über IT-Sicherheitsmaßnahmen für Unternehmen.

VON KARIN LEGAT

Sicherheit in der IT ist komplex. Über 50 Angriffsarten sind bereits klassifiziert und es werden immer mehr. »Cybercrime reicht von Phishing-Attacken mittels Mails über böswillige App-Anwendungen, Manipulation von Daten, Schadsoftware bis zum Cut von Produktionen«, zeigte Martin Rösler, Senior Director Forward Looking Threat Research bei Trend Micro, im Zuge des Webinars NextGen Security auf. 2010 wurden laut dem Bundeskriminalamt 4.223 Fälle von Cybercrime in Österreich angezeigt, 2019 waren es bereits 28.439. Hauptmotiv bilden zu 90 % finanzielle Verlockungen.

>> Risikofaktor Mensch <<

»Wenn sie nicht im unmittelbaren IT-Umfeld tätig ist, aktiviert die Hälfte der Mitarbeiter jeden sich bietenden Link«, spricht Thomas Blaschka, Solution Architekt Netzwerk und Security bei Bechtle, von erschreckend hohen Zahlen. »Die Menschen sind neugierig und klicken auf eine DHL-Benachrichtigung, obwohl nichts bestellt wurde, ebenso wie auf die Rechnungsaufforderung einer völlig fremden Firma.« Man kann zwar mit entsprechenden Sicherheitsmechanismen das Risiko einschränken, etwa dadurch, dass derartige Mails nicht bis zum User gelangen, aber 100 % Sicherheit gibt es nicht. Eine andere Möglichkeit ist die Deaktivierung der Links durch Antispam, Antimalware oder Mail-Protection.

Wenn Mitarbeiter im Homeoffice arbeiten, steigt die Cybergefahr durch fehlende Aktualisierung der Anwendungen, Missachtung von Richtlinien oder Installation von Schatten-Anwendungen auf den Geräten. Unternehmen müssen hier aktiv werden, das Bewusstsein schärfen, denn laut einer Umfrage des Jobportals Stepstone von Anfang Juni wollen fast zwei Drittel gerne nach der Krise weiter verstärkt im Homeoffice arbeiten.

Tipps fürs Homeoffice

Im Homeoffice, das zwei Drittel der Mitarbeiter nach der Corona-Krise gern weiter nutzen möchten, gilt:

- Jedes Gerät, insbesondere mobile Systeme, muss verschlüsselt sein, vor allem, wenn personenbezogene Daten natürlicher Personen damit verarbeitet werden.
- Ein Zugriff auf Firmennetzwerke darf ausschließlich über einen verschlüsselten VPN-Tunnel erfolgen. Lösungen mit TeamViewer oder ähnliche Plattformen sind zu vermeiden.
- Die gemeinsame Nutzung von PCs mit Familienangehörigen birgt ein enormes Risiko und muss vermieden werden, selbst wenn ein eigenes passwortgesichertes Profil eingerichtet wird.

Fotos: Trend Micro, Bechtle

»Wesentlicher Fixpunkt in der IT-Sicherheitsstrategie ist die Schaffung eines Notfallhandbuches für den Ablauf im Notfall. Es muss regelmäßig auf seine Plausibilität und Funktionalität geprüft werden«, informiert Thomas Blaschka.

Jedes vierte österreichische Unternehmen hat in den letzten drei Jahren bereits konkrete Angriffe auf Daten entdeckt.

wohl in Form professioneller Phishingkampagnen, um die Mitarbeiter zu sensibilisieren, bis hin zu klassischen Social-Engineering-Mechanismen. Als eine Lösung für mehr Sicherheit von Daten und Infrastruktur wurde beim Webinar VMware NSX genannt.

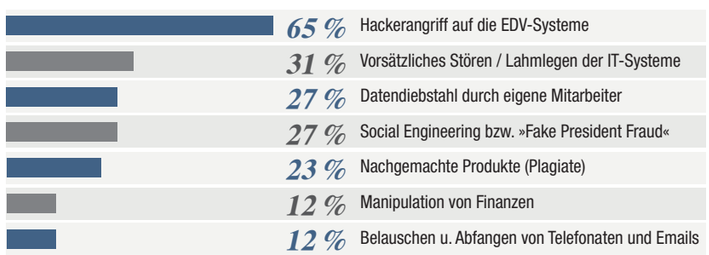
>> Virtuelle Fabrik <<

Im Rahmen von NextGen Security berichtete Trend Micro von einem sechs Monate laufenden Honeypot. Eine fiktive Fabrik wurde ins Netz gestellt, mit realer ICS-Hardware (Anm. Industrial Control System) und einer Mischung aus physischen Hosts und virtuellen Maschinen zum Betrieb der Fabrik, inkludiert waren mehrere speicherprogrammierbare Steuerungen, Human-Machine-Interfaces, separate Roboter- und Engineering-Workstations sowie ein Dateiserver, ebenso wie eine Schwachstelle. Der HMI-Computer wurde online über Virtual Network Computing ohne Kontrollzugriff verfügbar gemacht und das selbe Kennwort für mehrere Workstations verwendet. »Um weitere Angriffe anzulocken, haben wir unser System so aussehen lassen, als wäre es gehackt worden, indem durchgesickerte Informationen veröffentlicht wurden«, informiert Martin Rössler über das Projekt MeTech. Untersucht wurde, wer die Firma wie angreift. Ein Fazit war, dass ungesicherte Industrieumgebungen in erster Linie Opfer von herkömmlichen Cyberangriffen wurden. Der Honeypot wurde für das Mining von Kryptowährungen kompromittiert sowie durch zwei unterschiedliche Ransomware-Attacken ins Visier genommen. Zudem wurden seine Rechenkapazitäten für betrügerische Aktivitäten genutzt.

»Ein Ziel für Cyberangriffe bildet jeder. Betreiber kleinerer Fabriken und Industrieanlagen dürfen nicht davon ausgehen, dass Kriminelle sie in Ruhe lassen«, warnt der Trend Micro-Fachmann. Das Fehlen grundlegender Schutzmaßnahmen öffnet die Tür zu Ransomware- oder Kryptojacking-Angriffen mit schwerwiegenden Folgen.

»In der Vergangenheit wurde bei Cyberangriffen auf Produktionsanlagen vor allem herkömmliche Malware verwendet, die durch übliche Netzwerk- und Endpunktschutz-Lösungen gestoppt werden kann. Es ist jedoch wahrscheinlich, dass fortgeschrittene Angreifer zukünftig Operational Technology-spezifische Angriffe entwickeln, die dann unter dem Radar fliegen«, sagt Udo Schneider, IoT Security Evangelist Europe bei Trend Micro. Die beste Antwort darauf lautet: IIoT-spezifische Sicherheit. ■

Angriffsvektoren in der Wirtschaft



MOTIVATION für Cybercrime bildet in 90 Prozent der Fälle das liebe Geld. Quelle: Trend Micro

Verteidigung der Fabrik

IN ZUSAMMENARBEIT mit der Uni Mailand hat Trend Micro den Forschungsbericht »Attacks on Smart Manufacturing Systems: A Forward-looking Security Analysis« vorgestellt, der einen detaillierten Überblick über empfohlene Verteidigungs- und Eindämmungsmaßnahmen aufzeigt.

- Deep Packet Inspection zur Identifikation anomaler Payloads auf der Netzwerkebene
- Regelmäßige Integritätsprüfungen auf Endpunkten zum Aufzeigen geänderter Software-Komponenten
- Code-Signierung auf IIoT-Geräten zur Einbeziehung von Abhängigkeiten wie Bibliotheken von Drittanbietern
- Ausdehnung von Risikoanalysen auf Automatisierungssoftware
- Vollständige Chain of Trust für Daten und Software in intelligenten Fertigungsumgebungen
- Sandboxing und Privilegientrennung für Software auf Industriemaschinen