EINEN KLICK DEN HACKERN VORAUS SEIN

CYBERKRIMINALITÄT TRAF AUCH MARABU

Das Szenario klingt nach Science-Fiction, ist aber harte Realität in immer mehr Unternehmen. Angreifer verschaffen sich über das Internet unbemerkt Zugang zu den Firmenrechnern und damit auch den Daten, oftmals sensible Informationen wie Kundenstämme oder Produktionsdaten.

Diese Form der Industriespionage hat in den letzten Jahren deutlich zugenommen. Parallel steigt auch die Zahl der Fälle, in der die sogenannten Cyberkriminellen die Daten im Unternehmensnetzwerk mithilfe von Viren-Software verschlüsseln und die betroffenen Firmen dann auffordern für die Entschlüsselung der Daten ein Lösegeld, oft im 5– oder 6-stelligen Bereich, zu bezahlen.

Wie schaffen es die Straftäter immer wieder, in eigentlich sichere Netzwerke einzudringen und wie können sich Unternehmen hiergegen effektiv schützen? Hier sei vorangestellt, dass die Größe der Unternehmen mittlerweile keine Rolle mehr spielt. Die Angreifer gehen strategisch vor, spionieren ein Unternehmen erst aus und entscheiden dann, ob sich ein Angriff lohnt. Sofern dies der Fall ist, spielt die Größe des Unternehmens keine Rolle.
Viele Unternehmen haben mittlerweile nachgerüstet und verwenden Firewall-Systeme, die Zugriffe auf ein Netzwerk von außen abfangen oder Viren-Software auf den Arbeitsplatzrechnern der Mitarbeiter, die verhindern sollen, dass Schadsoftware unbemerkt ausgeführt wird. Trotz dieser Maßnahmen schaffen es die Angreifer aber immer öfter, sich unerlaubten Zugang zu verschaffen.

SCHWACHSTELLE MENSCH

Einfallstor und damit auch größte Schwachstelle von Unternehmen sind, das zeigen die Analysen der aktuellen Fälle, leider immer noch die Mitarbeiter. So schicken die Angreifer in der Regel manipulierte Mails, die scheinbar von bekannten Kontakten kommen oder verwenden manipulierte Webseiten, deren Besuch allein schon ausreicht, Schadsoftware auf einem Rechner zu installieren. Diese Methode nutzt den „Faktor Mensch“ aus – wenn ein bekannter Kontakt mir einen Link oder einen Anhang schickt, wenn Amazon mir eine Rechnung schickt, oder ich eine freundliche Bewerbung erhalte, der eine PDF anhängt, was kann da schon schiefgehen? Es sind aber genau solche Mails, die eigentlich aus dem Rahmen fallen, bzw. Verdacht wecken sollten.
Sicherheitsexperten gehen aufgrund der Entwicklungen mittlerweile davon aus, dass sich ein Angriff nicht verhindern lässt und die Verteidigungsstrategie im Unternehmen darauf aufbauen sollte, eine Ausbreitung der Schadsoftware im Unternehmen zu verhindern, in dem die betroffenen Systeme automatisiert „in Quarantäne“ genommen werden.
Was tun?

DAS BSI – BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK SIEHT DIE FOLGENDEN MASSNAHMEN ALS UNBEDINGTES MUSS AN:

- Regelmäßige Information und Sensibilisierung von Nutzern für die Gefahren durch E-Mail-Anhänge oder Links – einschließlich des Hinweises, auch bei vermeintlich bekannten Absendern (siehe auch gefälschte Absenderadressen) Dateianhänge oder Links bzw. über diese heruntergeladenen Dateien im Zweifel nur nach Rücksprache mit dem Absender zu öffnen (insbesondere auch keine Office-Dokumente). Nutzer sollten Auffälligkeiten umgehend an den IT-Betrieb und den IT-Sicherheitsbeauftragten melden.
- Zeitnahe Installation der von den Software-Herstellern bereitgestellten Sicherheitsupdates für Betriebssysteme und Anwendungsprogramme (insbesondere Web-Browser, Browser-Plugins, E-Mail-Clients, Officeanwendungen, PDF-Dokumentenbetrachter) – idealerweise automatisiert über eine zentrale Softwareverteilung.
- Einsatz zentral administrierter Antiviren-Software. Regelmäßige Prüfung, ob Updates von AV-Signaturen erfolgreich auf allen Clients ausgerollt werden.
- Regelmäßige Durchführung mehrstufiger Datensicherungen (Back-ups), insbesondere von Offline-Backups. Zu einem Back-up gehört immer auch die Planung des Wiederanlaufs und ein Test des Rückspielens von Daten.

- Regelmäßiges manuelles Monitoring von Logdaten, idealerweise ergänzt um automatisiertes Monitoring mit Alarmierung bei schwerwiegenden Anomalien.
- Netzwerk-Segmentierung (Trennung von Client-/Server-/Domain-Controller-Netzen sowie Produktionsnetzen mit jeweils isolierter Administration) nach unterschiedlichen Vertrauenszonen, Anwendungsbereichen und/oder Regionen.
- Fehler interner Nutzer stellen die größte Gefahr dar. Alle Nutzerkonten dürfen daher nur über die minimal zur Aufgabenerfüllung notwendigen Berechtigungen verfügen.

(Quelle: BSI)

Wesentlich für Unternehmen, die hier noch keine Strategie haben, ist es, sich mit dem zuständigen IT-Dienstleister abzustimmen und einen Plan für den Schutz auszuarbeiten und diesen auch kurzfristig umzusetzen. Zusätzlich sollte eine klare Backup-Strategie entwickelt werden, damit im Notfall die Daten schnell wiederhergestellt werden können. Dazu gehört auch die umfassende Dokumentation „lebenswichtiger" Prozesse im Unternehmen und klar definierte Notfall-Pläne für den Fall der Fälle.

BEISPIEL VIRUS EMOTET.

Eine der größten Bedrohungen stellte im letzten Jahr die Schadsoftware „Emotet" dar. Das Schadprogramm wird über Spam-Kampagnen verteilt und stellt eine akute Bedrohung für Unternehmen, Behörden und Privatanwender dar.
Die Schadsoftware liest Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern infizierter Systeme aus und nutzt diese Informationen zur weiteren Verbreitung des Virus:
Empfänger erhalten E-Mails mit echt wirkenden, jedoch frei erfundenen Inhalten von Absendern, mit denen sie kurz zuvor in Kontakt standen. Die korrekte Angabe der Namen und Mailadressen von Absender und Empfänger in Betreff, Anrede und Signatur lassen diese Nachrichten authentisch wirken. Wer jetzt den Dateianhang öffnet oder die verlinkte URL öffnet, lädt sich unbemerkt die schädliche Software auf den Rechner.
Einmal infiziert, lädt Emotet auf dem befallenen Rechner weitere Schadsoftware nach, beispielsweise den Trojaner Trickbot. Die Schadprogramme helfen beim Datendiebstahl und geben den Kriminellen die vollständige Kontrolle über das befallene System. Die Folge sind bisweilen große Produktionsausfälle, da ganze Unternehmensnetzwerke neu aufgebaut werden müssen.

BEISPIEL MARABU:

In der Nacht des 29.11.2019 wurde die Marabu GmbH & Co. KG Opfer einer gezielten Cyberattacke. Die Sicherheitsroutinen des Unternehmens haben daraufhin alle Systeme - auch bei Tochtergesellschaften - weltweit heruntergefahren. Hierdurch war das Unternehmen sechs Tage lang mehr oder weniger von der Außenwelt abgeschnitten, da neben E-Mail und Internet auch Telefone und Faxgeräte ohne Netzwerkanbindung nicht funktionierten.
Obwohl die gut ausgearbeiteten Notfallpläne und Sicherheitssysteme funktionierten, konnte nicht aufgehalten werden, dass Teile der Daten auf den Servern verschlüsselt und somit zunächst unbrauchbar wurden. Daraufhin wurde umgehend das Landeskriminalamt informiert, was permanent beratend zur Seite stand. Die Ermittlungen dauern bis heute an.
Für Marabu war es eine Grundsatzentscheidung, dass man nicht auf mögliche Lösegeldforderungen eingeht, sondern alles daransetzte, die Systeme aus eigener Kraft wiederherzustellen.
Der Druckfarbenhersteller rät heute anderen Firmen, eine Bilanz über ihre IT-Sicherheitssysteme zu ziehen und diese auf Wirksamkeit der Schutzmaßnahmen zu überprüfen. Erstellen Sie frühzeitig einen Notfallplan und testen Sie Ihr Backup. Stellen Sie sicher, dass dieses nicht im direkten Zugriff steht. Schulen Sie Ihre Mitarbeiter und Anwender und sagen Sie niemals, dass Sie „sicher“ sind, denn es gibt leider keine 100% IT-Sicherheit.