heise online heise+

Ein übergeordneter Schutzschirm

Wie sich Unternehmen vor immer komplexeren Cyberattacken schützen

Ransomware, Phishing, Spyware, Krypto-Jacking: Angriffe über das Internet sind für Unternehmen eine massive und permanente Bedrohung. Allein 68 Prozent der deutschen Industrie-Unternehmen waren laut einer Bitkom-Umfrage bereits Opfer von Cyberkriminellen, betroffen sind alle Betriebsgrößen und Branchen. Der Schaden ist mit 43 Milliarden Euro immens. Im schlimmsten Fall ist der Betrieb zeitweise lahmgelegt.

Die Cyber-Angreifer arbeiten effizient: 30.000 Webseiten werden jeden Tag gehackt, um über sie Schadcodes zu verbreiten. Experten und Sicherheitsfirmen warnen täglich vor neuen Gefahren. Aktuell gehören dazu gefälschte Bewerbungsanschreiben, in deren Anhängen sich Ransomware versteckt, oder Banking-Trojaner, die versuchen, sensible Bank-Daten vor allem kleiner und mittlerer Unternehmen abzugreifen. Innerhalb eines Jahres um 44 Prozent gestiegen ist auch die Zahl der Krypto-Jacking-Opfer, wie neulich bekannt wurde. Die Kriminellen kapern dafür die Server und Computer von Unternehmen und Privatanwendern, um Kryptowährungen wie Monero zu schürfen.

Nicht nur Konzerne und Privatnutzer sind von den Attacken betroffen. Die Kriminellen haben auch Behörden und kritische Infrastrukturen wie Stromnetze oder den Nahverkehr im Visier. Was solche Angriffe anrichten, zeigte sich in der US-Stadt Atlanta: Nach einer Attacke funktionierte unter anderem das WLAN am Flughafen eine Woche lang nicht mehr, und Bürger konnten Fahrscheine für die öffentlichen Verkehrsmittel und Parktickets nicht mehr online bezahlen.

Hinter den digitalen Überfällen stecken oft hochprofessionelle und organisierte Täter aus verschiedenen Ländern. Zum Beispiel soll die russische Hacker-Vereinigung „Sandworm“ laut Verfassungsschutz hinter einer Angriffswelle auf deutsche Medienunternehmen und europäische Organisationen stecken. Gleichzeitig werfen die USA China vor, Hacker mit dem Diebstahl geheimer Daten von Unternehmen und Behörden zu beauftragen.

Die Security-Herausforderungen steigen

In einer vernetzten Welt mit rapide wachsendem Datenvolumen steigt das Sicherheitsrisiko. 33 Zettabyte an Daten umfasste der globale Datenpool 2018, bis 2025 wächst er auf 175 Zettabyte an, sagt der Festplattenhersteller Seagate voraus.

sie in lokalen und Cloud-Datenbanken. Das erhöht die Angriffsfläche für Angreifer.

In der Industrie 4.0 arbeiten Maschinen und Anlagen zunehmend vernetzt. Sie alle sind potenzielle Einfallstore für Hacker, die über eine Attacke aus der Ferne den Ablauf im Unternehmen massiv stören können. Auch die vernetzten Geräte im Internet of Things sind Zielscheiben der Kriminellen: Jeder Sprachassistent und jede smarte Glühbirne ermöglichen den Zugang zu anderen Geräten und Daten im Heimnetzwerk. Eine Schwachstelle ist darüber hinaus jeder Router als Zentrale aller online-fähigen Geräte im Haus. Im Herbst 2018 etwa lockten mehr als 100.000 gehackte Router ihre Besitzer mithilfe von manipuliertem DNS auf Online-Banking-Betrugsseiten.

Mehr zum Thema:

- Bitkom-Umfrage: Attacken auf deutsche Industrie verursachten 43 Milliarden Euro Schaden
- Schutzschirm Blue Shield Umbrella
- Über diesen Beitrag

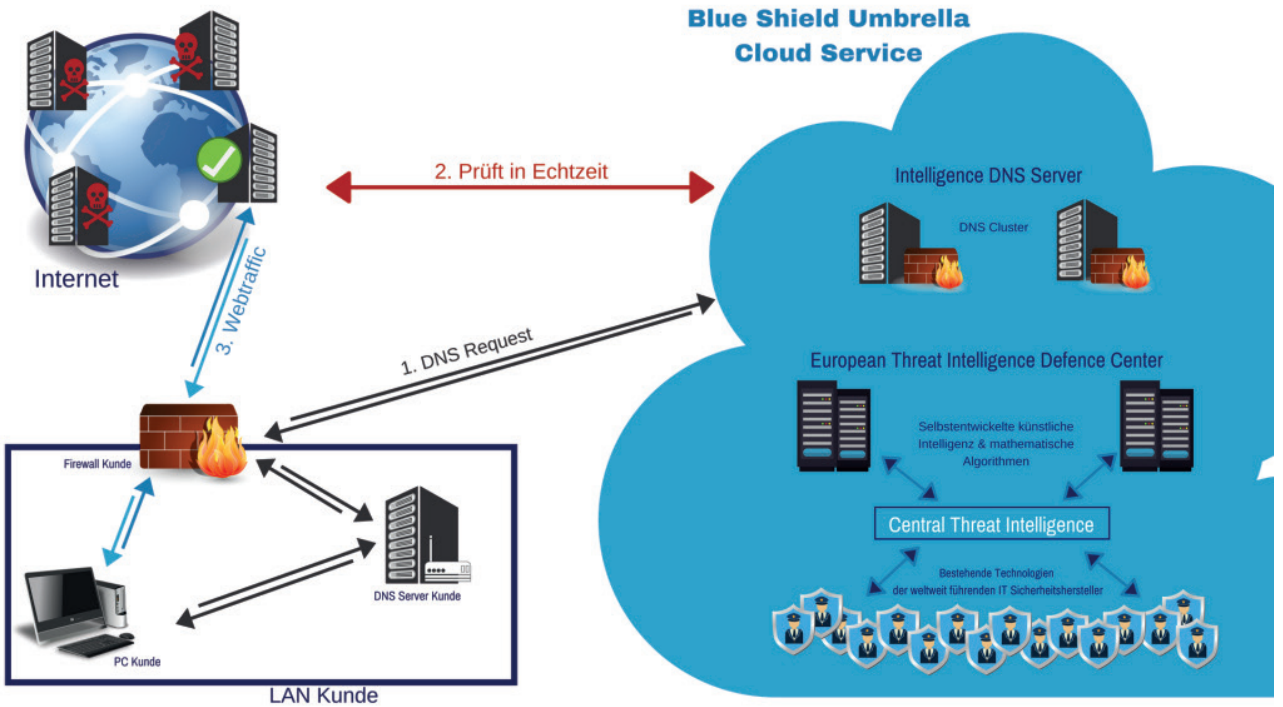
Warum herkömmliche Security-Konzepte nicht ausreichen

Die Herausforderung wird noch größer durch die Tatsache, dass Malware und Viren immer intelligenter arbeiten. Die Security-Experten von Blue Shield Security erwarten, dass Hacker schon 2019 zunehmend Künstliche Intelligenz (KI) nutzen, um Viren anzupassen und zu steuern. Das macht es herkömmlichen Security-Lösungen noch schwerer, die dadurch immer komplexeren Angriffe abzuwehren. Dazu kommt: Cyberkriminelle testen ihre Schadprogramme mit aktuellen Virenscannern und versuchen sie zu überlisten.

Die meisten Sicherheitslösungen nutzen ähnliche Methoden, um Gefahren zu erkennen und abzuwehren. Diese sind zwar erprobt, aber können oft nur zeitverzögert reagieren. Mithilfe von Signaturen werden beispielsweise Schadprogramme identifiziert. Die Verteilung der aktualisierten Signaturen an Anwender nimmt aber Zeit in Anspruch. Ein weiteres Problem: Die Mustererkennung greift nicht immer sofort, weil die Schadprogramme sich schnell verändern. Eine isolierte Sandboxing-Umgebung ermöglicht zwar, verdächtige Programme auszuführen, ohne dass sie das System beeinträchtigen können. Aber viele Viren erkennen, dass sie sich in einer Sandbox befinden, und reagieren erst wieder, wenn sie daraus entlassen werden.

Ein Lösungsansatz: der übergeordnete Schutzschirm Blue Shield Umbrella

Cyberkriminelle nutzen zwar ein breites Spektrum an Angriffsmethoden, die Wege zum Einschleusen ihrer Software sind aber ähnlich. Meist nutzen sie E-Mails mit Anhängen oder Links, gefälschte Webseiten sowie Drive-by-Attacken und manipulieren dabei die Namensauflösung des Domain Name Systems (DNS). Das DNS sorgt dafür, dass bei Eingabe eines Domain-Namens der zugehörige Host gefunden wird. Die Namensserver im LAN leiten alle Anfragen an Root-DNS-Server weiter und erhalten Antworten zurück. Ein manipulierter Link und Name führen dann zu einem kompromittierten Server. Virenscanner erkennen ihn nicht als bedrohlich.



Statt der Root-DNS-Server werden für die Namensauflösung ausschließlich sichere Server angefragt – die des hauseigenen Intelligence DNS Center (Grafik: Blue Shield)

Aber es gibt auch die Möglichkeit, ergänzend zu vorhandenen Sicherheitslösungen einen weiteren Schutzschirm aufzuspannen und so zu verhindern, dass bösartige Software überhaupt ins System gelangt. Es handelt sich um Software-as-a-Service, sie muss weder auf firmeninternen Systemen installiert noch gewartet oder aktualisiert werden. Ein solches System ist Blue Shield Umbrella: Statt der Root-DNS-Server werden für die Namensauflösung ausschließlich sichere Server angefragt – die des hauseigenen Intelligence DNS Center. Im Zentrum steht das European Threat Intelligence Defence Center, das zu 100 Prozent Eigentum von Blue Shield Security ist und von ihm betrieben wird. Rund um die Uhr werden dort in Echtzeit Mailserver und Webseiten analysiert, Gefahren errechnet und diese mithilfe von Künstlicher Intelligenz vorherzusagen versucht. Zusätzlich fragt das System IT-Sicherheitsmechanismen von Security-Herstellern weltweit ab und bezieht sie ein. Kompromittierte Server werden geblockt – und damit unbekannte Schadsoftware schon vor dem Eindringen in das Netzwerk abgewehrt.