Ein Unternehmen der

enviaM-Gruppe

E-Book

Cybersicherheit: Managed Services vs. Inhouse

enviaTEL

Das digitale Zeitalter ist allgegenwärtig. Die gesamte Wirtschaft steht vor unzähligen Herausforderungen, sich den schnelllebigen Veränderungen in kürzester Zeit anzupassen. Große, aber auch kleine und mittlere Unternehmen (KMU) sehen sich mit einer zunehmenden Gefahr durch die digitale Welt konfrontiert: der Cyberkriminalität. Das Whitepaper zeigt auf, welche Schwierigkeiten Unternehmen haben, eine interne Sicherheitslösung zu etablieren. Es wird auf den Problemfaktor Fachkräftemangel innerhalb der IT-Branche sowie den Faktor der Zeit und Faktor der Kosten eingegangen.

Eine Anleitung zu schnell umzusetzenden Securitymaßnahmen für KMU soll dabei helfen, den Mindestschutz zu gewährleisten. Um allerdings hohe Kosten in Personal, Wissen oder Software zu vermeiden, empfiehlt es sich, einen Managed Security Service Provider (MSSP) hinzuzuziehen.

Inhalt

1 Wie „Ubiquitous Computing“ die Welt verändert

Allmählich verschwimmen die Grenzen zwischen der digitalen und analogen Welt. Das digitale Zeitalter und die Arbeit mit dem Computer sind in der gesamten Wirtschaft omnipräsent. Alles ist vernetzt und „Ubiquitous Computing“ beschreibt diese Allgegenwärtigkeit der digitalen Informationsverarbeitung. Es gehört zum Alltagshandeln, dass sich Datennutzung und -verarbeitung über viele Endgeräte und Systeme gleichzeitig verteilen. Alles bündelt sich in einem gigantischen Kosmos der digitalen Transformation.

Vor wenigen Jahren konnten kritische Infrastrukturen in der IT-Anwendungslandschaft noch autonom und ohne ständige Überwachung durch die IT funktionieren.[1] In der Gegenwart kommt es immer mehr zu Angriffen aus der digitalen Welt. Die IT-Sicherheit ist nicht nur zum Handeln, sondern auch zum Umdenken aufgefordert. Es gilt, Cyberkriminalität, Cyberangriffe oder Cyberspionage abzuwenden. Für kleine und mittlere Unternehmen (KMU) können bei Erfolg selbst die einfachsten Angriffe eine Existenzbedrohung bedeuten. Die Schäden sind dabei individuell und gehen weit über die reinen finanziellen Verluste hinaus.

Mögliche Schäden durch Cyberangriffe für Unternehmen sind:

- **Wirtschaftliche Schäden:** Ein wirtschaftlicher Schaden entsteht durch die Kosten, die mit der Behebung und Reparatur beschädigter Systeme und dem Diebstahl von Unternehmensinformationen oder geistigem Eigentum einhergehen.
- **Reputationskosten:** Nach einem Cyberangriff, der aufgrund fehlender Sicherheitsmaßnahmen entstanden ist, ist es nicht selten, dass die Medien über entsprechende Sicherheitslücken im Unternehmen berichten. Zudem müssen Partner des Unternehmens ebenfalls über den Angriff informiert werden. Das führt zu einem Verlust an Vertrauen der aktuellen bzw. zukünftigen Kunden.
- **Regulierungskosten:** Die Strafen für Datenschutzverstöße sind wesentlich gestiegen, sodass ein Unternehmen auch mit hohen Bußgeldern oder Sanktionen rechnen muss.

1: Vgl. Fraunhofer (2020): Strategie- und Positionspapier Cybersicherheit 2020. Herausforderungen für die IT-Sicherheitsforschung. Fraunhofer-Verbünde IUK-Technologie. Verteidigungs- und Sicherheitsforschung. 53 Seiten. Zugriff: https://www.iese.fraunhofer.de/content/dam/iese/de/dokumente/Fraunhofer-Strategie-und_Positionspapier_Cyber-Sicherheit2020.pdf, 8. Januar 2021, 10:30 Uhr.

Im Rahmen einer Studie des Beratungsunternehmens „techconsult" waren bereits 66 Prozent der befragten Unternehmen Opfer eines Cyberangriffs. Jedes zweite davon sogar mehrfach.[2] 2019 ist allein in Deutschland ein finanzieller Schaden von fast 90 Millionen Euro durch Cyberkriminalität entstanden. Im Vergleich zum Vorjahr ist das eine Steigerung von über 60 Prozent.

Deutschlands Mittelständler sind ein beliebtes Ziel für „Hacker", weil es hier nicht nur eine hohe Anzahl an Patentanmeldungen gibt, sondern damit verbunden auch eine Vielzahl an innovativen Geschäftsideen.

1.1 Cyberkriminalität professionalisiert sich

Die steigende Nutzung von „Cloud Services", die zunehmende Vernetzung und wachsende Abhängigkeiten von Technologie und Automatisierung führen dazu, dass Cyberkriminalität weltweit aggressiver und vielfältiger wird. Laut Bundeskriminalamt stieg die von der Polizei registrierte Zahl an Vorfällen der Internetkriminalität. Hauptziel der Angriffe sind Unternehmen.

Großunternehmen scheinen aufgrund des hohen Kapitals ein lukratives Ziel zu sein, allerdings hat Informationssicherheit in solchen Unternehmen oberste Priorität, weshalb sich die Überwindung der Sicherheitsmaßnahmen für Angreifer oft als zu aufwendig gestaltet. Nicht zuletzt deshalb rücken zunehmend KMU in das Visier der Täter. Die Nutzung von veralteter Software, fehlende Kenntnisse über IT-Sicherheit und kleine Budgets für Security-Maßnahmen erleichtern Angreifern ihre Taten. KMU legen im Gegensatz zu Großunternehmen oftmals weniger Wert auf Richtlinien und Vorgaben, beispielsweise die Umsetzung der Datenschutz-Grundverordnung.[3]

> Während der Covid-19-Pandemie ist das Cybercrime-Ökosystem nochmals strukturierter und professioneller geworden. Das liegt unter anderem an dem Umzug vieler Arbeiternehmer vom Büro ins Homeoffice.

2: Vgl. Proofpoint c/o GlobalTax GmbH (2020): Zwei von drei Unternehmen bereits Opfer von Cyberkriminalität. Zugriff: https://www.netzwoche.ch/news/2020-10-19/zwei-von-drei-unternehmen-bereits-opfer-von-cyberkriminalitaet, 8. Januar 2021, 10:50 Uhr.

3: Vgl. Ratgeber Datenschutz-Praxis, Oliver Schonschek (2019): So sieht eine IT-Sicherheitsrichtlinie aus. Zugriff: https://www.datenschutz-praxis.de/tom/so-sollte-eine-sicherheitsrichtlinie-aussehen/, 21. Januar 2021, 16:30 Uhr.

Cyberkriminalität ist zu einem Beruf geworden. Die Akteure begehen die Taten nicht allein, sondern schließen sich in spezialisierten Gruppen zusammen. Diese organisieren sich wie die Unternehmen, auf die sie abzielen. Die bekanntesten Praktiken sind u. a. Malware-as-a-Service sowie DDos-as-a-Service. Die häufigsten Vorfälle waren Netzwerk- und Anwendungsanomalien, gefolgt von Benutzerkontenanomalien und Malware-Angriffen. Ransomware-Akteure (Angreifer, die ihre Opfer mittels Erpressungs- oder Verschlüsselungstrojaner infiltrieren) haben ihren Ansatz weiterentwickelt, indem sie beispielsweise nicht nur die Verfügbarkeit von Daten, sondern auch deren Vertraulichkeit monetarisiert haben.

Bei einem Cyberangriff sehen Unternehmen nicht nur ihre Daten durch Trojaner verschlüsselt, sondern sind zunehmend auch der Gefahr ausgesetzt, dass einige davon öffentlich bekannt gegeben werden. Diese Methode ermöglicht die Kompromittierung von unzähligen Unternehmen und die Erpressung von Lösegeld in Millionenhöhe.

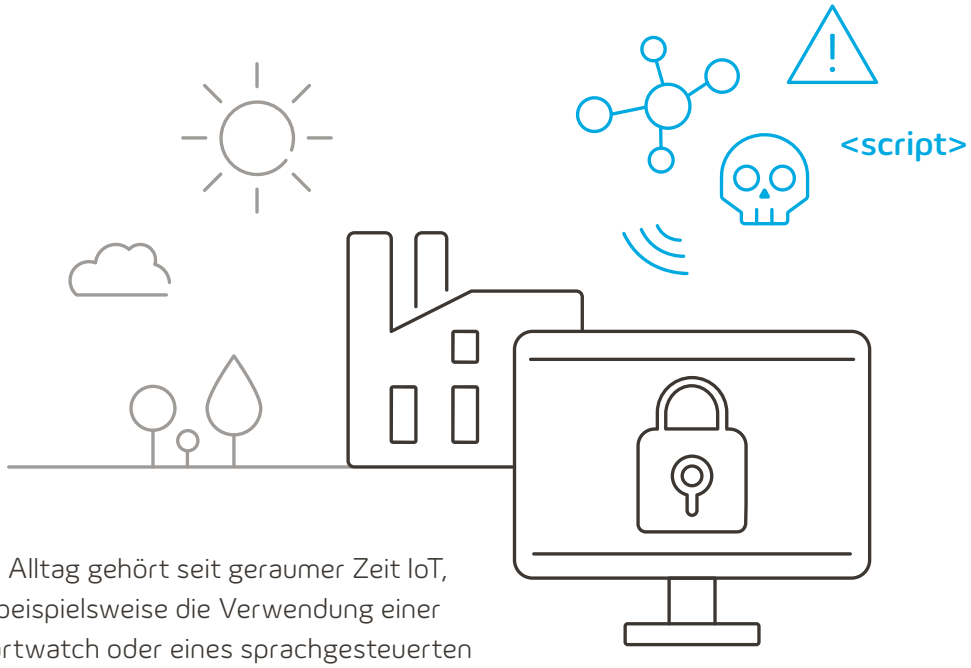
1.2 Neue Angriffsarten übergehen Schutzmechanismen von herkömmlichen Firewalls, Anti-Viren-Programmen und „Intrusion-Detection-Systemen"

Netzwerksicherheitslösungen werden von Tag zu Tag anspruchsvoller und bieten ein schnell wachsendes Schutzniveau auf immer effizientere und kostengünstigere Weise. Cyberkriminelle finden trotzdem immer neue Wege in die vermeintlich am besten geschützten IT-Infrastrukturen. Die heutige Cyberbedrohungs-Landschaft ist polymorpher Natur, da sie sich ständig ändert. Hacker nutzen immer innovativere Methoden.

Besonders betroffen sind Unternehmen mit älteren Firewalls, die nicht den Inhalt von Netzwerkpaketen untersuchen, sondern Datenpakete lediglich anhand von IP-Adresse und Ports herausfiltern können. Mit der sogenannten „Deep Packet Inspection" (DPI) lassen sich bösartige Codes, Malware und andere Sicherheitsbedrohungen zuverlässig erkennen und leicht aus dem Verkehr herausfiltern, bevor sie Schaden anrichten können.

Die Aufgabe einer Firewall besteht jedoch nicht nur darin, eingehenden Datenverkehr zu überprüfen, sondern auch darin, sicherzustellen, dass das Netzwerk nicht unerwartet vom jeweiligen Benutzer verlassen wird. Eine alarmierende Anzahl von Unternehmensfirewalls ist so konfiguriert, dass sie zwar den eingehenden Datenverkehr überprüfen, die Daten, die das Netzwerk verlassen, jedoch nicht im Auge behalten. Der Einstieg in das Netzwerk kann sich zwar als Herausforderung erweisen, aber sobald sich Angreifer im Netzwerk befinden, können sie so Daten nach Belieben abfließen lassen. Wenn die Firewall nicht überprüft, was das Netzwerk verlässt, werden Datenlecks nicht erkannt.

Hinzu kommt, dass nur bei Benutzung einer aktiven Firewall der entsprechende Schutz gewährleistet werden kann. Wenn Mitarbeiter unbedacht die Netzwerksicherheitsrichtlinien umgehen, sind sie sich über die resultierenden Auswirkungen oft im Unklaren. Daher ist es maßgebend, die Mitarbeiter in Schulungen zu sensibilisieren, die Wichtigkeit von Sicherheitsrichtlinien zu verdeutlichen und deren Umsetzung lückenlos durchzusetzen. Wechseln Mitarbeiter in ein offenes WLAN, sollte das nur unter Verwendung einer VPN-Verbindung geschehen, prinzipiell ist jedoch von der Nutzung nicht-vertrauenswürdiger Netzwerke abzuraten.



Zum Alltag gehört seit geraumer Zeit IoT, wie beispielsweise die Verwendung einer Smartwatch oder eines sprachgesteuerten Smart-Lautsprechers. Die Industrie 4.0 vereint bei Produktionen die intelligenten Informations- und Kommunikationssysteme der IoT-Geräte mit dem Digitalisierungsdrang der Wirtschaft. Infolgedessen begrüßen viele Unternehmen internetfähige Geräte – von sehr unterschiedlicher Komplexität – am Arbeitsplatz. Das Spektrum reicht von Cloud-angereicherten Zugangskontrollsystemen bis hin zu intelligenten Beleuchtungs- und Heizungslösungen. Ohne angemessenen Schutz bergen IoT-Systeme jedoch zahlreiche Risiken. Viele der verwendeten IoT-Geräte erhalten selten oder keine Sicherheitsupdates, verwenden meist schwache Verschlüsselung und senden gesammelte Daten oft unkontrolliert zurück zu ihren Cloud-Plattformen. Sie sind daher ein beliebtes Ziel von Hackern, da sie meist leicht angegriffen und gekapert werden können und sich oft jahrelang unerkannt im Netzwerk aufhalten.

Solche Geräte werden im Anschluss oft dazu genutzt, um verteilte Angriffe (Distributed Denial-of-Service) auf andere Netzwerk-Ziele durchzuführen. Es ist wichtig, dass sie hinter der Firewall sowie einem Intrusion-Prevention-System (IPS) liegen und in alle anderen Cybersicherheitslösungen eingebunden sind.