CYBER DEFENSE FÜR DEN MITTELSTAND
DIE BEDROHUNG NIMMT ZU

Geschäftsblockaden, Datendiebstahl und Erpressung aus dem Internet nehmen stetig zu. Dennoch sind viele mittelständische Unternehmen nicht oder nicht gut gegen solche Attacken gerüstet. „Warum sollte gerade mein Unternehmen angegriffen werden?“, fragen sich viele. Die Mittel sind knapp, und so lange nichts passiert ist, scheint ja alles in Ordnung zu sein.

Wirklich? Die Wirtschaft vernetzt sich immer mehr. Wertschöpfungsprozesse gehen längst über Unternehmensgrenzen hinaus. Der deutsche Mittelstand als Innovationsträger ist ein attraktives Angriffsziel. Und gleichzeitig wird es immer leichter, zielgerichtete Angriffe auszuführen: Hacker sind international vernetzt und kaum dingfest zu machen. Werkzeuge zur Erstellung von Schadsoftware werden mittlerweile mehr oder minder offen zum Kauf angeboten. Daher sprechen Experten davon, dass es keine Frage mehr ist, OB ein Unternehmen angegriffen wird, sondern WANN. Und haftbar für Schäden durch Cyberkriminalität ist die Geschäftsführung.

VIELE MITTELSTÄNDISCHE UNTERNEHMEN UNTERSCHÄTZEN DIE BEDROHUNG

DIE ANGRIFFE WERDEN IMMER RAFFINIERTER

Herkömmliche Schutzkonzepte wie Firewalls, Intrusion Prevention Systeme und Virenschutzprogramme reichen heutzutage nicht mehr aus. Sie dienen als Basisschutz, können aber nicht mit dem komplexen Vorgehen der Angreifer mithalten, da ständig neue, unbekannte Schadprogramme und Angriffsstrategien entwickelt werden. Auftragshacker führen zielgerichtete und professionelle Angriffe („Advanced Persistent Threats“) aus. Sicherheitslücken in Programmen werden ausgenutzt und IT-Systeme unerkannt manipuliert. Angreifer bewegen sich zum Teil monatelang unerkannt im Netzwerk ihrer Opfer, bis sie deren „Kronjuwelen“ entdeckt und unbemerkt entwendet haben.

Dabei sind die Motive vielfältig: Wirtschaftsspionage, die Sperrung von Datenzugriff, um Lösegeld zu erpressen, Sabotage, um nur einige zu nennen.

DOCH UNTERNEHMEN KÖNNEN SICH SCHÜTZEN

Moderne Abwehrmethoden wie Cyber Defense für den Mittelstand von Telekom schützen Unternehmen auf aktuellstem Wissenstand: Das Verhalten von Netzwerk und IT-Systemen wird kontextbezogen und in Echtzeit überwacht, Angriffe können sehr viel schneller erkannt und Gegenmaßnahmen ergriffen werden, bevor Schaden entsteht. Dies erfolgt z. B. durch die Sammlung und Analyse von Log- und Netzwerkdaten durch ein „Security Incident and Event Management“-System (SIEM) bis zur Behandlung von Sicherheitsvorfällen unter Einbindung des „Security Operation Center“ (SOC). Informationen aus einer Vielzahl von Security-, Netzwerk- und IT-Systemen werden im SIEM zusammengetragen und automatisiert in Echtzeit analysiert. Festgelegte Regeln, die genau auf die Situation und den Schutzbedarf des jeweiligen Unternehmens zugeschnitten sind, lösen Alarme aus, sobald etwas nicht stimmt. Ein genau festgelegter Arbeitsprozess leitet den Alarm an Experten, um die Situation zu beurteilen und, wenn nötig, Gegenmaßnahmen einzuleiten.

CYBER DEFENSE FÜR DEN MITTELSTAND

Nur die wenigsten mittelständischen Unternehmen haben die Mittel und das Personal, um eine moderne, umfassende Sicherheitsarchitektur aufzubauen und zu unterhalten. In der Regel werden Einzellösungen von verschiedenen Herstellern für Teilbereiche der IT-Sicherheit eingesetzt: Firewalls, Virenscanner und Intrusion Prevention Systeme haben unterschiedliche Management-Systeme, Sicherheitsberichte müssen mühsam aus verschiedenen Quellen erstellt werden.

Im Gegensatz dazu reduziert der Service „Cyber Defense für den Mittelstand“ aus dem Hause Telekom Kosten und Komplexität. Auf Basis der Unified Security Managegement (USM)-Plattform des weltweit renommierten Herstellers AlienVault hat Telekom ein umfassendes Angebot zusammengestellt, mit allen relevanten Maßnahmen:

UNSER ANGEBOT

Wir bieten: von der Beratung über die Integration bis hin zu Betriebsleistungen alles aus einer Hand. Dabei stehen zwei Stufen zur Verfügung:

1. Cyber Defense Services mit Basisbetrieb
Die zentrale Komponente von Cyber Defense für den Mittelstand wird in sicheren Telekom Rechenzentren oder beim Kunden vor Ort bereitgestellt und betrieben. Das Sammeln der von den Kundensystemen gesendeten Daten erfolgt durch Sensoren, die in der jeweiligen Kundenumgebung installiert werden. Bereitstellung der zentralen Hardware, Lizenzen, Überwachung, Wartung (Update und Patching) sowie Störungsbeseitigung auf System- und Anwendungs-Level führt dabei die Deutsche Telekom durch.

Die Leistungen im Detail:

- Bereitstellung der zentralen Komponenten, Anbindung der Kundennetze, Bereitstellung der Agenten-Software
- 24x7 Betrieb der zentralen Cyber Defense für den Mittelstand-Plattform
- Störungsmanagement
- Service, Monitoring und Service Reporting
- Beratungs-Leistungen werden ergänzend und nach Kundenwunsch angeboten

2. Cyber Defense Services mit erweitertem Betrieb
Unsere speziell dafür ausgebildeten Experten übernehmen hierbei die Überwachung und Auswertung auftretender Ereignisse und deren Verarbeitung. Dies umfasst die Echtzeit Erkennung und Bewertung von Sicherheitsvorfällen, um den Kunden mit validen und relevanten Informationen zu versorgen.

Als zusätzliche Leistung können Sie Unterstützung bei der Bekämpfung von Sicherheitsvorfällen oder Bedrohungen erhalten.

LEISTUNGEN ALS MANAGED SERVICE

- Automatisierte Auswertung von Firewall-Protokolldateien, um die Ausbreitung von Netzwerk-Würmern frühzeitig zu erkennen
- Erkennung der Ausnutzung von Systemschwachstellen durch das integrierte Network Intrusion Detection-System (NIDS)
- Bruteforce-Angriffe auf Windows- und Linux- Systeme erkennen
- Unerwünschte Kommunikation von Trojanern mit Command and Control Servern erkennen
- Schwachstellen-Erkennung mittels integriertem Vulnerability Scanner
- Passive und aktive Asset Discovery Erfassung
- Einfache Integration von zu überwachenden Windows und Unix Systemen
- Compliance-Berichte für PCI, HIPAA, FISMA, ISO27001
- Generierung von Security Reports im PDF Format
- Echtzeit-Überblick über den Security Status des Untenehmens
- Out-of-the-Box-Security-Dashboards
- Zentrale Speicherung von Protokoll-Daten der überwachten Systeme

KONTAKT
Persönlicher Kundenberater
Freecall 0800 33 05400
www. telekom.de/geschaeftskunden

HERAUSGEBER
Telekom Deutschland GmbH
53262 Bonn

Stand 3/2015 | Änderungen und Irrtümer vorbehalten | tiktay

ERLEBEN, WAS VERBINDET.