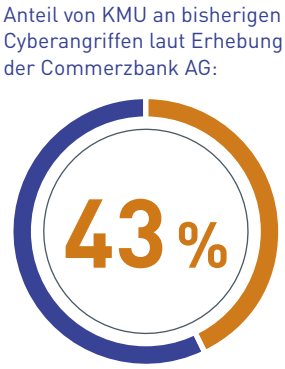
IT-SICHERHEIT IM MITTELSTAND:

Zielscheibe für Cyberkriminelle – **wie sich schützen?**

Kleine und mittlere Unternehmen (KMU) waren 2024 besonders attraktive Ziele für Cyberkriminelle. Laut einer aktuellen Studie des Digitalverbands Bitkom waren fast 80 % der deutschen Unternehmen in den letzten zwölf Monaten von Cyberangriffen betroffen, wobei besonders kleine Unternehmen ins Visier geraten sind … | VON RENÉ BENACHOUR

Bild: nxtgenit



Grafik: Computern im Handwerk

Eine Untersuchung der Commerzbank zeigt, daß 43 % der KMU bereits Opfer eines Cyberangriffs wurden, was die besonders hohe Gefährdung des Sektors unterstreicht. Zudem bestätigte das Bundesamt für Sicherheit in der Informationstechnik (BSI), daß mehr als 40 % der Cyberangriffe auf Unternehmen im KMU-Sektor verübt werden. Diese Unternehmen sind aufgrund mangelnder IT-Ressourcen und veralteter Sicherheitslösungen oft unzureichend gegen die zunehmenden Bedrohungen abgesichert.

Die Ursachen für die besonders hohe Gefährdung von KMU liegen in mehreren Bereichen. Zum einen fehlt es vielen Unternehmen an spezialisierten IT-Sicherheitsteams, die ihre Netzwerke regelmäßig auf Schwachstellen überprüfen und auf neue Bedrohungen reagieren können. Zum anderen setzen viele KMU auf veraltete oder nicht mehr zeitgemäße Sicherheitslösungen, die mit den immer komplexeren Angriffsmethoden nicht mehr mithalten können. Hinzu kommt, daß viele Unternehmen ihre Mitarbeiter nicht ausreichend auf die Gefahren aus der Cyberwelt vorbereiten. Laut einer Untersuchung von Kaspersky war die unsachgemäße Nutzung von IT-Ressourcen durch Mitarbeiter bei 39 % der Cyberangriffe weltweit ein bedeutender Faktor menschlichen Versagens. Auch ein Bericht des Weltwirtschaftsforums aus dem Jahr 2021 zeigt, daß menschliches Versagen bei 95 % der IT-Probleme eine Rolle spielt, sei es durch das Öffnen von Phishing-Mails oder das unbewußte Weitergeben von vertraulichen Informationen. Diese sogenannte „menschliche Schwachstelle“ ist nach wie vor die größte Bedrohung für die Sicherheit von Netzwerken in KMU.

Die Bedrohungen der Zukunft: Was KMU 2025 erwarten können

Die Bedrohungen für KMU werden im Jahr 2025 zunehmend komplexer. So hat sich in den letzten Monaten ein neuer Trend abgezeichnet: Cyberkriminelle setzen zunehmend auf die sogenannte Ransomware-as-a-Service (RaaS). Mit diesem Modell können auch technisch weniger versierte Kriminelle Angriffe starten und für einen Anteil am Lösegeld potentielle Opfer erpressen. Ein weiteres Risiko, das Unternehmen 2025 ins Auge fassen müssen, sind Angriffe mit künstlicher Intelligenz (KI). Hierbei kommen selbstlernende Algorithmen zum Einsatz, die es Angreifern ermöglichen, ihre Angriffsstrategien kontinuierlich zu verbessern und ihre Opfer gezielt zu attackieren. Laut einer Untersuchung von Gartner wird bis 2026 mehr als die Hälfte aller Angriffe auf Unternehmen auf KI-basierte Techniken zurückzuführen sein. Auch die Cloud-Sicherheit bleibt ein zentrales Thema, da immer mehr Unternehmen ihre Daten in der Cloud speichern. Das BSI warnt, daß Angreifer

vermehrt Sicherheitslücken in Cloud-Diensten ausnutzen werden, wenn Unternehmen nicht ihre Sicherheitsvorkehrungen verstärken.

Automatisierung als Schlüssel zur Cyberabwehr

Angesichts dieser steigenden Bedrohungen können manuelle Sicherheitsmaßnahmen nicht mehr ausreichend sein. Die Automatisierung von Cybersicherheitsprozessen hat sich als ein entscheidender Schritt erwiesen, um Bedrohungen schnell und effizient zu erkennen und abzuwehren. Automatisierte Systeme sind rund um die Uhr aktiv und bieten den Vorteil, daß sie keine Verzögerungen durch menschliches Eingreifen haben. Sie reagieren in Echtzeit und reduzieren menschliche Fehler, was für Unternehmen, die kontinuierlich Risiken ausgesetzt sind, von entscheidender Bedeutung ist. Ein weiterer Vorteil der Automatisierung ist die Reduktion von Fehlalarmen. Während statische Schutzmaßnahmen oftmals zu ungenauen Blockierungen führen, ermöglichen dynamische, automatisierte Systeme eine präzise Identifikation und Reaktion auf Bedrohungen, die das Unternehmen tatsächlich betreffen.

Antwort auf die Bedrohungen der Zukunft

Cybersicherheitslösungen, die auf die speziellen Bedürfnisse von KMU zugeschnitten sind, nutzen fortschrittliche Technologien wie künstliche Intelligenz (KI) und maschinelles Lernen (ML), um Bedrohungen in Echtzeit zu analysieren und automatisch zu neutralisieren. So bietet z. B. NxtFireGuard von NxtGenIT maßgeschneiderte Blocklisten, die auf die individuellen Bedrohungen eines Unternehmens abgestimmt sind und sich kontinuierlich an die sich verändernde Bedrohungslandschaft anpassen.

Die Integration in bestehende Sicherheitslösungen ist einfach, sodaß Unternehmen ihre Schutzmaßnahmen nicht nur erweitern, sondern auch optimieren können. Durch die Automatisierung der Bedrohungsabwehr wird nicht nur die Effizienz gesteigert, sondern es wird auch ein Beitrag zur globalen Cybersicherheit geleistet. Automatisierte Prozesse melden verdächtige IP-Adressen und potentielle Angreifer in Echtzeit, was den Schutz über die Unternehmensgrenzen hinaus verstärkt. Mit solchen Lösungen können KMU ihre Sicherheitsstrategie auf ein neues Niveau heben, ohne ihre Ressourcen erheblich zu belasten.

In einer Zeit, in der die Bedrohungen immer komplexer werden, ist eine dynamische und automatisierte Sicherheitslösung der Schlüssel, um sowohl aktuellen, als auch zukünftigen Angriffen vorzubeugen. <<

Noch Fragen?
https://www.nxtgenit.de/

SOPHOS:

Cyberschutz im Handwerk auf Konzernniveau

Kleinere und mittelständische Betriebe haben nicht selten die Herausforderung, sich mit Themen befassen zu müssen, die nicht zu ihrer Kernaufgabe gehören. Dazu zählt insbesondere die Cybersicherheit – nicht zuletzt, weil Cyberattacken immer häufiger und trickreicher werden und weil auch im Handwerk die IT elementar für viele Arbeitsabläufe ist. Die Digitalisierung der Unternehmensorganisation, der Auftragsbearbeitung oder der vernetzten Maschinen bieten den Cyberkriminellen enorme Angriffsflächen. Die bittere Wahrheit: Laut dem Sophos State of Ransomware Report werden 47 Prozent der Unternehmen mit einem Umsatz von weniger als 9,2 Millionen Euro von Ransomware-Banden angegriffen.

Es gibt aber auch gute Nachrichten. Der Security-Anbieter Sophos hat mit „Cybersecurity Divide“ eine Initiative gestartet, die Unternehmen jeder Größe mit einer Kombination aus Technologie und menschlicher Serviceleistung zur bestmöglichen Cybersicherheit verhilft. Das Ziel: Betriebe mit einem hoch wirksamen Cyberschutz auszurüsten, der mit dem Schutzniveau großer Unternehmen schritthält – jedoch mit geringerer Komplexität und deutlich günstiger als Konzernlösungen.

Das integrierte Sicherheits-Ökosystem von Sophos ist weltweit bei über 600.000 Unternehmen im Einsatz und vereint intelligente technische Lösungen mit Künstlicher Intelligenz und externen Security-Spezialisten. Die technische Security etabliert den intelligent gesteuerten Grundschutz, während die Künstliche Intelligenz das gesamte Netzwerk zusätzlich nach Anomalien durchkämmt. Externe Spezialisten werden automatisch über alle Verdachtsfälle in Echtzeit informiert und treten umgehend in Aktion, untersuchen den Vorfall, beseitigen die Schadprogramme und schließen die Lücken, durch die sich Cyberkriminelle eingeschlichen haben. Damit verfügen auch kleinere und mittlere Unternehmen über eine Cybersicherheit auf Konzernniveau. <<

Weitere Infos:
https://www.sophos.com/de-de/small-and-medium-business