ActualTech Media

Hewlett Packard Enterprise

Sicherheit in KMUs kann schwierig (und kostspielig) sein

Ed Tittel

INHALT

THEMA

HPE hilft kleinen und mittleren Unternehmen (KMUs) angesichts immer größerer und gefährlicherer Bedrohungen wie Ransomware, Phishing, Datenlecks, Hacking und mehr bei der Einrichtung und Aufrechterhaltung der betrieblichen Sicherheit.

KMUs brauchen Hilfe von Experten, um Personalengpässe und Qualifikationslücken zu schließen, da langsame Reaktionszeiten kostspielig sein können. In diesem Beitrag wird untersucht, wie HPE KMUs dabei hilft, diese Probleme anzugehen.

Highlights:

- Umstellung von reaktiver, statischer Sicherheit auf intelligente, adaptive Sicherheit
- Schließung von IT-Sicherheitslücken mit Abdeckung am Edge, in der Cloud und On-Premises
- Definition einer Sicherheitsstrategie, die Sicherheit, Compliance, IT Continuity und Disaster Recovery umfasst
- Integration von Sicherheit in die KMU-Struktur

Die digitale Welt von heute ist fast schon beängstigend. Alle Unternehmen und Organisationen sehen sich mit den gleichen komplexen und abschreckenden Sicherheitsbedrohungen konfrontiert, auch kleine und mittelständische Unternehmen (KMUs). Wie jede aktuelle Sicherheitsumfrage zeigt, sehen sich Unternehmen aller Größenordnungen mit einer immer größeren Anzahl unterschiedlicher Bedrohungen konfrontiert und bieten eine immer größer werdende Angriffsfläche für böswillige Angriffe.

> **In einer Umgebung, in der das IT-Personal nur schwer mit den Entwicklungen mithalten kann, können die meisten KMUs nur auf Sicherheitswarnungen reagieren, anstatt Bedrohungen proaktiv und präventiv zu handhaben und potenzielle Schwachstellen zu beseitigen.**

Laut der Forrester Studie „2020 State of Security Operations" waren 79 % der Unternehmen in den letzten 12 Monaten mit einer Sicherheitsverletzung irgendeiner Art konfontiert. Datenschutzverletzungen, so die Studie, sind und bleiben ein ständiges Problem für alle Unternehmen. Darüber hinaus stehen Sicherheitsteams und ihre Arbeitgeber vor großen technologischen Herausforderungen. Viele dieser Herausforderungen resultieren aus komplexen oder isolierten Tools, die Ineffizienzen verursachen und zu unzureichenden Sicherheitsergebnissen führen. Dieselbe Studie zeigt zudem die aktuellen Top 5 bei den Sicherheitsbedrohungen nach der Art der Bedrohung auf:

1. Ransomware: Rogue-Software, die Geschäftsdaten und -systeme verschlüsselt, die ohne Bezahlung für die Entschlüsselung nicht wiederhergestellt werden können – ohne Erfolgsgarantie.
2. Phishing: Links in E-Mails, auf Webseiten oder in sozialen Medien, die unvorsichtige Benutzer auf bösartige Seiten führen, auf denen Kennwörter und Anmeldedaten gestohlen werden (und mehr).
3. Datenlecks: Unerlaubte Mittel, durch die Geschäftsdaten an Sicherheitsvorkehrungen im Unternehmen vorbei in die falschen Hände gelangen.
4. Hacking: Technische und Social-Engineering-Angriffe auf IT-Infrastrukturen mit dem Ziel, die Kontrolle zu übernehmen, den Zugriff oder Service zu verweigern und Daten, geistiges Eigentum oder Geld zu stehlen.
5. Insider-Bedrohung: Angriffe von ehemaligen oder aktuellen, oft verärgerten Mitarbeitern, die Insider-Kenntnisse nutzen, um an Geschäftsdaten, geistiges Eigentum oder finanzielle Werte zu gelangen.

Die meisten Unternehmen (laut Forrester 83 %) verfügen über eine Art 24/7-Sicherheitsabdeckung. Zu oft fehlt es aber an der richtigen Technologie und am richtigen Personal, um mit der ständig wachsenden Anzahl und Schwere von Cyberangriffen Schritt zu halten. Viele Unternehmen haben tatsächlich große Mühe, mit der Menge an Sicherheitswarnungen, die sie täglich verarbeiten müssen, Schritt zu halten.

Kein Mangel an Sicherheitsproblemen in KMUs

Kleine und mittlere Unternehmen sind besonders anfällig für Sicherheitsprobleme, da sie nur über wenig IT-Personal verfügen und die Sicherheitsexpertise entweder kaum vorhanden oder das Sicherheitsteam oft stark überlastet ist. In einer Umgebung, in der das IT-Personal nur schwer mit den Entwicklungen mithalten kann, können die meisten KMUs nur auf Sicherheitswarnungen reagieren, anstatt Bedrohungen proaktiv und präventiv zu handhaben und potenzielle Schwachstellen zu beseitigen.

Dadurch sind KMUs dem hohen Risiko ausgesetzt, dass es zu katastrophalen Schäden oder Verlusten kommen kann. Laut Ponemon Institute beliefen sich die durchschnittlichen Kosten einer Datenschutzverletzung im Jahr 2020 auf 3,86 Mio. US-Dollar. Für einen kleinen Betrieb entscheidet ein Verlust in dieser Größenordnung über Überleben oder Scheitern. Darüber hinaus können einige Angriffsarten, wie z. B. Ransomware, ein KMU buchstäblich an den Rand des Ruins treiben, weil es seine Geschäfte nicht mehr ausführen kann. Einen solchen Angriff als echte Katastrophe zu bezeichnen, ist keineswegs übertrieben. KMUs brauchen einen durchdachten Sicherheitsschutz, um auch potenzielle rechtliche und regulatorische Risiken zu vermeiden, die Datenschutzverletzungen bei Kundendaten ebenso mit sich bringen können wie erhebliche finanzielle Strafen und Rufschädigungen für das Unternehmen.

Tatsächlich kann eine langsame Reaktionszeit auf einen Sicherheitsangriff oder eine Datenschutzverletzung eine echte Katastrophe für KMUs bedeuten. Die Opportunitätskosten für entgangene Geschäftschancen, kombiniert mit den Kosten für Reparatur, Wiederherstellung und Berichterstattung (und potenzielle Folge-Audits) und mehr, belasten das Geschäftsergebnis erheblich. Kurz gesagt: eine gute Sicherheitsstrategie kann teuer und ressourcenintensiv sein, aber die Kosten, die aus einer fehlenden oder unterdurchschnittlichen Strategie resultieren, können noch deutlich höher ausfallen. Auch die Funktionsfähigkeit und sogar das Überleben des Unternehmens können dadurch bedroht sein.

Die Unternehmensgrenzen in KMUs öffnen sich immer weiter

Es gab einmal eine Zeit, da konnten sich KMUs gezielt auf ihre Unternehmensgrenzen konzentrieren. Durch den Schutz dieser Grenzen wurden die meisten Sicherheitsbedenken ausgeräumt und die meisten Risiken beseitigt. Heutzutage sind Daten und Apps überall zu finden, wodurch es schwieriger wird, alles zu verfolgen und zu sichern. Durch die aktuellen Pandemie-Regeln arbeiten die Mitarbeiter meistens remote, was bedeutet, dass jedes einzelne genutzte Gerät geschützt werden muss. Da das Internet ein wichtiges Bindeglied zwischen Benutzern und Anwendungen und Services ist, ist eine sichere Kommunikation wichtiger denn je. Gleiches gilt für sichere Speicherkomponenten und Server, sowohl vor Ort als auch in einer oder mehreren Clouds (heutzutage meist mehrere Clouds). Sicherheit und Schutz werden also dann schnell interessant, wenn die Assets, Anwendungen und Mitarbeiter eines Unternehmens orts- und zeitunabhängig arbeiten.

HPE Sicherheitslösungen

HPE kann KMUs bei der wichtigen Umstellung von reaktiven, statischen und isolierten Sicherheitstools und -techniken auf intelligente, adaptive Sicherheitsplattformen in der digitalen Welt von heute unterstützen. Mit den Sicherheitslösungen von HPE können KMUs bestehende Sicherheitslücken durch die Abdeckung vom Edge, über die Cloud bis On-Premises schließen – alles unter einem einheitlichen und kohärenten Sicherheitsschirm. Hierfür bietet HPE folgendes Leistungsspektrum:

- Datenorientierte Sicherheit: Baut auf bewährten Methoden nach NIST-Standard auf, um genutzte, ruhende und fließende Daten zu schützen (die die Anforderungen der US-Regierung und der DSGVO (Datenschutzgrundverordnung) der EU erfüllen). Diese datenorientierte Sicherheit bietet eine wirksame Verschlüsselung und Tokenisierung, um gestohlene Daten für Angreifer unbrauchbar zu machen.
- Zero Trust-Sicherheit: Zero Trust ist ein philosophischer Ansatz für das Identitäts- und Zugriffsmanagement, bei dem standardmäßig keine Benutzer- oder Softwareaktion als vertrauenswürdig angesehen wird. Also müssen alle Benutzer, Geräte und Anwendungsinstanzen ihre Identitäten und Berechtigungen schlüssig nachweisen, bevor der Zugriff erlaubt wird.
- DevSecOps: Bei diesem Ansatz werden Sicherheitsteams und -konzepte in einen formalen Entwicklungsprozess eingebunden. So wird sichergestellt, dass das Thema Sicherheit frühzeitig und häufig entlang der gesamten App-Lieferkette (Entwurf, Aufbau, Test, Bereitstellung, Wartung) berücksichtigt wird und nicht einfach am Ende der Entwicklung an ein „fertiges“ System oder einen Service angehängt wird. Die Sicherheit wird während der Entwicklung und Bereitstellung durch eine Reihe von DevSecOps Best-Practices berücksichtigt (**Abbildung 1**).

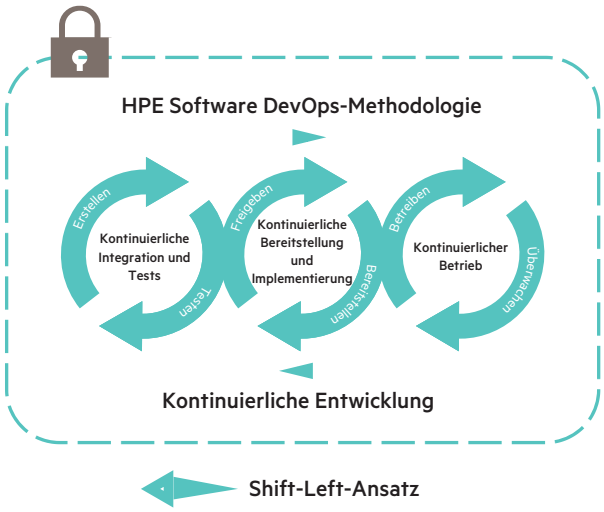

Abbildung 1: DevSecOps erweitert die zugrunde liegenden Konzepte von DevOps, um die Mentalität aufzubauen, dass jeder Einzelne für die Sicherheit verantwortlich ist.

HPE Trusted Supply Chain Initiative

Um die Anforderungen von Kunden mit hohen Sicherheitsanforderungen und anspruchsvollen Nutzungsszenarien zu erfüllen, stellt HPE eine Trusted Supply Chain bereit. Zu diesen Kunden gehören Benutzer aus dem öffentlichen Sektor und der US-Regierung, die Produkte aus den USA mit nachweisbarer Cybersicherheit bevorzugen. Die Sicherheit wird in die Lieferkette integriert, indem zusätzliche verstärkte Sicherheitsfunktionen eingebunden werden. HPE Mitarbeiter werden dann beauftragt, die Produkte während des Fertigungsprozesses zu überwachen, um alle Teile zu prüfen, die Montage zu beobachten und sicherzustellen, dass die verpackten Geräte bis zur Annahme der Lieferung durch den Kunden manipulationssicher bleiben. HPE bietet ein exklusives Silicon Root of Trust-Konzept, bei dem Sicherheit auf Chipebene in Industriestandard-Server eingebettet wird, und unterhält Sicherheitskontrollen in der gesamten Lieferkette, um strikte Sicherheit auf Hardware-Ebene zu etablieren und zu erhalten.

HPE berücksichtigt das Thema Sicherheit natürlich auch bei der eigenen Produktentwicklung und -lieferung, indem eine formal dokumentierte, häufig geprüfte sichere Lieferkette verwendet wird (siehe: **„HPE Trusted Supply Chain Initiative“**).

> **HPE kann KMUs bei der wichtigen Umstellung von reaktiven, statischen und isolierten Sicherheitstools und -techniken auf intelligente, adaptive Sicherheitsplattformen in der digitalen Welt von heute unterstützen.**

Die HPE PointNext Consulting Services helfen KMUs zudem, ihre Sicherheitsstrategie zu prüfen, definieren und verfeinern. Experten helfen dabei, dass die Sicherheitsrichtlinien den Sicherheitsanforderungen im gesamten Unternehmen gerecht werden und gleichzeitig die Compliance-Anforderungen in Bezug auf Datenschutz, Vertraulichkeit und Datensicherheit erfüllen. Dieselben Experten können KMUs auch helfen, erschwingliche und effektive Optionen für Business Continuity und Disaster Recovery als Teil einer intelligenten und adaptiven Sicherheitsplattform zu integrieren, die KMUs implementieren wollen. In diesem Zusammenhang können diese Experten Ihrem KMU Sicherheitsentwürfe zur Verfügung stellen, auf denen Ihre eigenen Entwürfe und Implementierungen basieren. Und sie können Ihnen dabei helfen, diese Entwürfe durch alle Phasen wie Test, Pilotprojekt und Implementierung in der Produktionsumgebung zu begleiten.

Eingebaute Sicherheit am Edge

HPE arbeitet sehr eng mit den KMUs zusammen, um hohe Sicherheit im gesamten Unternehmen zu gewährleisten. Das bedeutet, dass ihre Remote-Mitarbeiter sicher sind und die Sicherheit am Edge, On-Premises und in Hybrid-Cloud-Umgebungen eingebettet und einbezogen wird. Dieser Ansatz bindet die Sicherheit in die gesamte IT-Infrastruktur in all ihren Implementierungen und Erscheinungsformen ein. HPE Edge enthält also integrierte Sicherheitsfunktionen, damit das Edge-Computing-Leistungsspektrum – wie intelligente Arbeitsbereiche, IoT-Umgebungen, virtuelle Desktop-Infrastrukturen und Servicebereitstellung für Microsoft (Teams, Exchange, Microsoft 365), VMware, Linux VMs und mehr – von Beginn an und nachhaltig sicher bleibt – von der Nutzung bis zur Weiterentwicklung im Lauf der Zeit. Das Gleiche gilt für HPE Rechenzentrums- und Cloud-/Hybrid-Cloud-Lösungen wie HPE GreenLake, HPE InfoSight und viele andere HPE Lösungen.

> **HPE arbeitet sehr eng mit den KMUs zusammen, um hohe Sicherheit im gesamten Unternehmen zu gewährleisten.**

Auf der HPE Seite „Security and Digital Protection Services“ finden Sie weitere Informationen zu Sicherheitsentwürfen, das HPE Sicherheits portfolio, Fallstudien und mehr.