ActualTech MEDIA

Hewlett Packard Enterprise

Den Sicherheitsrisiken immer einen Schritt voraus

Ed Tittel

INHALT

Die Cloud verändert alles ... auch die Sicherheit 2

So kann HPE (mit seinen Partnern) die IT schützen 3

- HPE Sicherheit beginnt bei den Servern 3
- HPE Sicherheitslösungen 4
- Jenseits der Lösungen: Professionelle Beratungsleistungen 4

ÜBERBLICK

In diesem Kurzbericht erfahren Sie, wie HPE und seine Partner kleine und mittelständische Unternehmen dabei unterstützen, Sicherheitsrisiken zu vermeiden. Solche Unternehmen müssen in der Lage sein, Bedrohungen und Schwachstellen, die potenzielle Risiken darstellen, zu erkennen, sie nach Schweregrad zu ordnen und Pläne zur Risikominderung und zur Durchführung von Maßnahmen zu erstellen. Dies erfordert das ständige Bemühen, mit einer sich ständig verändernden Bedrohungslandschaft Schritt zu halten.

Highlights:

- Abstimmung der Sicherheitsstrategie auf die Unternehmensziele
- Aufbau einer auf Sicherheit ausgerichteten Unternehmenskultur
- Überwachung möglicher Angriffspunkte und proaktives Gegensteuern zur Verhinderung von Hackerangriffen

Wenn es um Cybersecurity geht, ist das alte Sprichwort „Vorbeugen ist besser als heilen“ besonders zutreffend. Das liegt daran, dass die Kosten für die Beseitigung der Folgen eines Sicherheitsproblems oder einer Sicherheitsverletzung heutzutage so hoch sind, dass sie für die meisten Unternehmen, insbesondere für kleinere Betriebe, eine existenzielle Bedrohung darstellen.

Deshalb ist es so wichtig, die Gefahren, die von Sicherheitsbedrohungen und Schwachstellen ausgehen können, zu erkennen und zu antizipieren, wenn nicht sogar unverzichtbar. Letztlich geht es um Risikomanagement, was Folgendes bedeutet:

- Wenn Bedrohungen und Schwachstellen bekannt werden, besteht der erste Schritt darin, diejenigen zu **identifizieren**, die tatsächliche Risiken für das Unternehmen darstellen, und ihre potenziellen Auswirkungen und Folgen zu bewerten.
- Bei den risikobehafteten Bereichen ist es wichtig, **Prioritäten** zu setzen, so dass die Bereiche mit den höchsten Kosten oder den schlimmsten Folgen zuerst angegangen werden, und so weiter, in abnehmender Reihenfolge.
- Für Bereiche, die ein entsprechendes Risiko bergen, sollten Unternehmen **Risikominderungs- und Aktionspläne** aufstellen, um sie anzugehen.

In der Praxis bedeutet dies vor allem für Unternehmen, die zu klein sind, um eine eigene Sicherheitsabteilung einzurichten, dass sie eine Art Bedrohungsanalyse- und Abhilfedienst abonnieren. Tatsächlich können HPE und seine Partner im Rahmen eines umfassenden Sicherheitsserviceangebots bei solchen Maßnahmen unterstützend mitwirken, etwa bei der Identifizierung, Priorisierung und Beseitigung von Risiken.

Die Cloud verändert alles ... auch die Sicherheit

In dem Maße, wie Unternehmen Cloud-Abonnements und -Dienste einführen, finden auch neue und schwierige Bedrohungsvektoren Eingang in das Sicherheitsbild eines Unternehmens. Daher ist es von entscheidender Bedeutung, die Sicherheitsvorkehrungen zu verbessern und Maßnahmen zu ergreifen, um die Sicherheitslage und die Cyber-Resistenz des Unternehmens zu verbessern. Die folgenden Maßnahmen können Unternehmen bei der Erreichung dieser Ziele helfen:

- **Stimmen Sie Ihre Sicherheitsstrategie auf die Unternehmensziele ab:** Durch das Verständnis der Diskrepanzen zwischen Unternehmens- und Cybersecurity-Prioritäten können die Unternehmensleitung und die verschiedenen Interessengruppen damit beginnen, beide Strategien aufeinander abzustimmen, um sicherzustellen, dass die Hauptprioritäten fokussiert und die Ressourcen und Budgets entsprechend zugewiesen werden. Wichtig ist, dass sich die Unternehmensleitung über die Prioritäten einig ist und dass die Risikoprofile klar verstanden werden.
- **Bauen Sie eine auf Sicherheit ausgerichtete Unternehmenskultur auf:** Eine Unternehmenskultur, in der Sicherheit an erster Stelle steht, ist ein wichtiger Schritt, um in einer Welt voller Unsicherheit und Risiken erfolgreich zu sein. Der Schutz lebenswichtiger Ressourcen geht uns alle an. Es ist wichtig, in die Sensibilisierung der Mitarbeiter zu investieren, da diese eine wichtige Quelle für Cyber-Risiken darstellen und ein gemeinsames Vorgehen gegen Cyber-Bedrohungen für Ihr Unternehmen von Vorteil ist.
- **Identifizieren Sie Ihre Angriffsflächen und beheben Sie Schwachstellen, bevor Hacker sie finden:** Die Analyse von Cyber-Schwachstellen, auch Sicherheitstests oder Pen-Tests genannt, ist ein Testverfahren zur Bewertung der Sicherheitslage Ihres Unternehmens (siehe **Abbildung 1**). Es identifiziert Schwachstellen, bevor ein Angreifer sie ausnutzen kann. Dieser Prozess bietet Einblicke in die Risiken, denen die Vermögenswerte der Organisation aus externer und interner Sicht ausgesetzt sind. Es hilft zudem, potenzielle Sicherheitslücken zu erkennen, bevor formale Bewertungen der Einhaltung von Vorschriften oder Audits durchgeführt werden. Um die Sicherheitslage in Ihrem Unternehmen zu verbessern, ist es außerdem wichtig, umsetzbare Pläne zur Risikominderung zu entwickeln. Zu diesem Zweck können erfahrene Partner (wie HPE und seine Partnerunternehmen) die Lücken in den Cyber-Kompetenzen Ihres Unternehmens schließen und Schwachstellen abschwächen.

Die vier Stufen eines Penetrationstests

Abbildung 1: Die vier Phasen der Penetrationstests, auch bekannt als Pen-Tests

Erläuterung der Terminologie

Notfallwiederherstellung: Beschreibt Dienste und Systeme, die es einem Unternehmen ermöglichen, selbst im Falle einer Katastrophe oder einer vollständigen Unterbrechung des Zugangs und der Dienste zum normalen Betrieb zurückzukehren.

Ransomware: Eine Art von Malware, die Unternehmen den Zugang zu ihren Systemen und Daten verwehrt, indem sie alles verschlüsselt, sodass nichts mehr funktioniert. Kriminelle behaupten, dass durch die Zahlung eines Lösegelds alles in den Zustand vor dem Angriff zurückversetzt wird, aber das FBI rät davon ab, Lösegeld zu zahlen, da dies nicht immer der Fall ist.

Virtualisierte und containerisierte Anwendungen und Daten: Anwendungen und Daten, die in virtuellen Maschinen oder Containern — häufig in der Cloud — ausgeführt werden, in der Regel als Teil eines nutzungs- und verbrauchsbasierten Computing-Modells.

Vom Edge bis zur Cloud: Bezieht sich auf Computing-Ressourcen und Daten, die sich in Rechenzentren oder Serverräumen vor Ort im Unternehmenskern, am Netzwerk-Edge an entfernten Standorten oder auf einer oder mehreren Cloud-Plattformen (z. B. Amazon Web Services, Microsoft Azure, Google Cloud Platform) befinden können.

Hybride und Multi-Cloud-Szenarien: Bei einer hybriden Cloud werden lokale und cloudbasierte Computing-Ressourcen in eine einzige Umgebung für die Abwicklung von Computing-Aufgaben integriert. Multi-Cloud bedeutet dasselbe, außer dass es sich dabei um zwei oder mehr Cloud-Plattformen handelt. Die meisten modernen Unternehmen arbeiten in hybriden Multi-Cloud-Umgebungen und versuchen, Arbeitslasten und Daten dort zu platzieren, wo es aus Kosten-, Sicherheits- und Leistungssicht am sinnvollsten ist.

Es ist wichtig, dass sich die Unternehmensleitungen über die Prioritäten einig sind und dass die Risikoprofile klar definiert werden.

So kann HPE (mit seinen Partnern) die IT schützen

Wie eine schnelle Prüfung zeigt, sind die Cybersecurity-Lösungen von HPE umfassend, innovativ und robust. Die Sicherheitsmaßnahmen beginnen auf der Hardware-Ebene und erstrecken sich bis hin zu den Benutzern und Systemen am Netzwerk-Edge. Die Hauptaufgabe besteht darin, Sicherheitsinformationen zu sammeln und zu analysieren, um mit der Bedrohungslage Schritt zu halten, Systeme und Dienste im betrieblichen Einsatz zu sichern und Kunden bei der Verwaltung und Minimierung von Sicherheitsrisiken zu beraten (und zu unterstützen).

Die Cybersecurity-Lösungen von HPE sind umfassend, innovativ und robust. Die Sicherheitsfunktionen beginnen auf der Hardware-Ebene und erstrecken sich bis hin zu den Benutzern und Systemen am Edge.

HPE SICHERHEIT BEGINNT BEI DEN SERVERN

HPE ist als Anbieter der weltweit sichersten Server nach Industriestandard bekannt. Die ProLiant-Serverfamilie hat dank dieser besonderen Eigenschaften zahlreiche Preise und Auszeichnungen erhalten:

- **Schützen:** Die Systeme vermeiden Angriffe auf Hardware- und Firmware-Ebene durch eine vertrauenswürdige Siliziumbasis (Root of Trust), TPM-Erweiterungen (Trusted Platform Module), mehrere Stufen der Manipulationssicherheit und zusätzliche HPE-Innovationen wie die iLO-Firmware (Integrated Lights Out) zur Förderung von „Security-First“-Funktionen.
- **Erkennen:** Eine breite Palette von Innovationen erkennt und wehrt Bedrohungen während der Laufzeit ab, einschließlich Boot-Integritätsprüfungen, bei denen iLO potenziell (oder tatsächlich) gehackten Firmware-Code löscht und nach Möglichkeit durch eine bekannte gültige Kopie ersetzt. Wenn eine Reparatur nicht möglich ist, wird das System nicht gebootet (bietet einen Pre-Boot-Schutz gegen Rootkits und andere gefährliche Firmware-basierte Angriffe).

- **Wiederherstellen:** Robuste Funktionen zur schnellen und einfachen Wiederherstellung von Systemen in ihrem letzten bekannten, funktionsfähigen Zustand, dank manipulationssicherer, verschlüsselter Backups und sicherer Wiederherstellungsmechanismen.

Zerto

Im Jahr 2021 schloss HPE die Übernahme von Zerto ab, einem Unternehmen, das sich auf Notfallwiederherstellung, Ransomware-Wiederherstellung und Multi-Cloud-Mobilitätslösungen spezialisiert hat. Zerto gehört jetzt zu HPE und bietet kontinuierliche Datensicherung und -wiederherstellung für virtualisierte und containerisierte Anwendungen und Daten vom Edge bis zur Cloud. Mit Zerto können Unternehmen innerhalb weniger Minuten den Zustand wiederherstellen, der nur Sekunden vor einem Angriff bestand, und so langwierige und kostspielige Unterbrechungen und Datenverluste vermeiden. Zerto bietet eine höhere Verfügbarkeit bei deutlich geringerem Verwaltungsaufwand als herkömmliche Datensicherungslösungen. Zudem macht das vereinheitlichte, skalierbare und automatisierte Datenmanagement von Zerto die Workload- und Datenmobilität über verschiedene Clouds hinweg zum Kinderspiel. Darüber hinaus bietet Zerto kontinuierlichen Datenschutz für Unternehmen, die eine Hybrid-Cloud-Strategie anwenden, und umfasst Disaster Recovery as a Service (DRaaS) mit einem Netzwerk von über 350 Managed Service Anbietern. Besuchen Sie die HPE/Zerto-Seite, um mehr darüber zu erfahren, wie Ihr Unternehmen Datenverluste und Anwendungsausfallzeiten so gut wie möglich vermeiden kann.

HPE SICHERHEITSLÖSUNGEN

Die Sicherheitstools, -technologien und -lösungen von HPE beruhen alle auf drei zentralen Ansätzen in den Bereichen Konzeption, Entwicklung, Herstellung und Wartung. Diese lassen sich am besten wie folgt beschreiben:

- **Datenorientierte Sicherheit:** Sicherheitsmaßnahmen dienen in erster Linie dem Schutz von Daten, insbesondere von sensiblen Daten (personenbezogene Daten, Konten und Kennwörter, Finanz-, Gesundheits- oder andere gesetzlich geschützte Daten usw.). Dies steht in direktem Zusammenhang mit dem darauf folgenden Ansatz, bei dem es darum geht, wer zu welchem Zweck Zugang zu Systemen und Daten erhält.

> **Die Einbindung erfahrener Partner (wie HPE und seine Partnerunternehmen) kann Lücken in den Cyber-Kompetenzen Ihres Unternehmens schließen und Schwachstellen beseitigen.**

- **Zero Trust-Sicherheit:** Das National Institute of Standards and Technology (NIST) beschreibt Zero Trust (ZT) mit folgendem Zitat: „Niemals vertrauen, immer prüfen.“ ZT zielt auf den Schutz von Daten und Diensten ab, sollte aber auch alle Ressourcen (Geräte, Infrastrukturelemente, Anwendungen sowie virtuelle und cloudbasierte Ressourcen) und Subjekte (Benutzer, Anwendungen, Dienste und Systeme) umfassen. Grundsätzlich geht ZT davon aus, dass Angreifer immer zugegen und aktiv sind. Daher wird niemandem stillschweigend vertraut, und die Risiken für Ressourcen und Geschäftsfunktionen werden stets analysiert und bewertet. Die Überprüfung der Identität bei allen Zugriffsanfragen ist eine Schlüsselstrategie, ebenso wie die Anwendung des „Prinzips der geringsten Privilegien“ (auch bekannt als PLP), was bedeutet, dass nicht mehr Privilegien gewährt werden, als die Personen benötigen, um ihre Arbeit zu erledigen.
- **DevSecOps:** Einfach ausgedrückt handelt es sich um eine Erweiterung des DevOps-Konzepts, bei dem Entwickler (und Support-Mitarbeiter wie Tester, Dokumentatoren und Ausbilder) zusammen mit dem Betriebspersonal (Administratoren, technischer Support und Techniker oder Troubleshooter vor Ort) in einer einzigen Organisation mit gemeinsamen Zielen zusammengefasst werden. DevSecOPs geht noch einen Schritt weiter und integriert das Sicherheitsteam in den gesamten Entwicklungslebenszyklus, sodass die Sicherheit während der Konzeptions-, Entwicklungs-, Test-, Wartungs- und Stilllegungsphasen im IT-Betrieb Berücksichtigung findet.

JENSEITS DER LÖSUNGEN: PROFESSIONELLE BERATUNGSLEISTUNGEN

HPE Pointnext Services unterstützen kleine und mittelständische Unternehmen bei der Prüfung, Definition und Optimierung ihrer Sicherheitsstrategien. Pointnext bietet professionelle Unterstützung bei der Formulierung von Sicherheitsrichtlinien und der

Erfüllung von Compliance-Anforderungen in Bezug auf Datenschutz, Vertraulichkeit und Datensicherheit. Zudem werden Unternehmen, deren Ressourcen oder Know-how begrenzt sind, bei der Integration kostengünstiger und effektiver Lösungen für die Aufrechterhaltung des Betriebsprozesses und die Notfallwiederherstellung unterstützt. Pointnext hat sich darauf spezialisiert, Unternehmen bei der Erstellung von Sicherheitsplänen zu unterstützen, um Sicherheitsdesigns und -implementierungen fest in der Praxis (und im Rahmen des Budgets) zu verankern. Pointnext Services bieten außerdem eine durchgängige Unterstützung bei Test-, Pilot- und Produktionseinsätzen. Letztendlich kann Pointnext Unternehmen dabei unterstützen, die Sicherheit in der gesamten Organisation zu verankern: bei Remote-Mitarbeitern, am Edge, vor Ort und in hybriden, Multi-Cloud-Umgebungen.

Schutz der Lieferkette

HPE betreibt eine vertrauenswürdige Lieferkette (Trusted Supply Chain, TSC), um Kunden mit hohen, überdurchschnittlichen Sicherheitsanforderungen oder Nutzungsszenarien zu bedienen. Zu den repräsentativen Kunden dieser Lieferkette gehören Organisationen und Behörden der US-Regierung und des öffentlichen Sektors, die Produkte „Made in USA“ mit nachprüfbarer Produktsicherheit erwerben müssen. Die Sicherheit wird in der TSC auf zwei wichtige Arten berücksichtigt. Zum einen enthalten solche Produkte strenge Sicherheitsvorkehrungen, die sie fälschungssicher, wenn nicht gar manipulationssicher machen sollen. Zum anderen überwacht HPE die gesamte Lieferkette, genehmigt alle Komponenten, überwacht die Montage und hält die verpackten Waren sicher (und manipulationssicher), bis die Kunden die Lieferung annehmen.

Project Aurora bietet eine vollständige Sicherheitsarchitektur mit neuen eingebetteten und integrierten Sicherheitslösungen, beginnend auf Chipebene. Erfahren Sie, wie Project Aurora in der Lieferkette beginnt und eine nicht veränderbare Vertrauenskette bis zur Infrastruktur, das Betriebssystem, die Softwareplattform und die Workloads aufbaut – ohne Signaturen, signifikante Leistungseinbußen oder Anbieterabhängigkeit.

Die Sicherheitstools, -technologien und -lösungen von HPE basieren auf drei zentralen Ansätzen in den Bereichen Konzeption, Entwicklung, Herstellung und Wartung.

HPE und seine Partnerunternehmen bieten eine breite Palette sorgfältig ausgearbeiteter Sicherheitslösungen an, die kleinen und mittelständischen Unternehmen helfen, Risiken zu verwalten, ihre Systeme und Daten zu schützen und mit der komplexen und unübersichtlichen Sicherheitslandschaft von heute zurechtzukommen. Besuchen Sie die HPE-Seite mit den IT-Lösungen für kleine und mittelständische Unternehmen, um mehr darüber zu erfahren. Bedenken Sie außerdem, dass HPE und seine Partner über die Pointnext Services Organisation auch Coaching, Beratung, Unterstützung und Services anbieten können, um kleineren Unternehmen dabei zu helfen, die Sicherheit und den Schutz zu erhöhen.