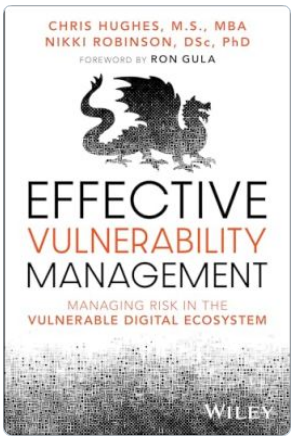
getabstract
compressed knowledge

Bewertung 9

Qualitäten
Umsetzbar
Augenöffner
Praktische Beispiele



Buch oder Hörbuch kaufen

Wirksames Schwachstellenmanagement

Risikomanagement in einem anfälligen digitalen Ökosystem

Chris Hughes und Nikki Robinson • Wiley © 2024 • 288 Seiten

Management / Risikomanagement / IT-Sicherheit

Take-aways

- Die Anlagenverwaltung ist für das Schwachstellenmanagement entscheidend.
- Unternehmen brauchen ein automatisiertes Patch-Management-Protokoll.
- Einzelpersonen und Unternehmen sollten Systeme zur digitalen Regulierung einrichten.
- Schwachstellenmanagement erfordert höchste Wachsamkeit und kontinuierliche Überwachung.
- Weisen Sie Schwachstellen bestimmte Werte zu, damit Sie sie priorisieren können.
- Cyberangreifer nutzen zahlreiche Schwachstellen aus.
- Mithilfe von öffentlich zugänglichen Informationen können Sie herausfinden, welchen Bedrohungen Sie ausgesetzt sind.
- Die Mitwirkung von Menschen ist im Schwachstellenmanagement entscheidend.
- Führungskräfte sollten beim Aufbau ihrer Organisation die Sicherheit im Blick haben.

Rezension

2022 hingen 60 Prozent des weltweiten Bruttoinlandsprodukts von digitalen Technologien ab. Daher machen sich viele Führungskräfte Gedanken über die möglichen Auswirkungen einer Cyberattacke. Der kritische Punkt, so die Cyberexperten Chris Hughes und Nikki Robinson in ihrem Buch, ist die Anfälligkeit digitaler Systeme – und wie wir damit umgehen. Klar ist: In einer Geschäftswelt, in der nichts ohne Internet geht, müssen Einzelpersonen und Organisationen sich um Sicherheitslücken kümmern, bevor ein Problem auftritt oder ein Angriff stattfindet. Das Buch gibt hierfür wertvolle Anregungen.

Zusammenfassung

Die Anlagenverwaltung ist für das Schwachstellenmanagement entscheidend.

Zwar sind digitale Umgebungen heutzutage höchst unterschiedlich, doch jedes Schwachstellenmanagement muss eine Anlagenverwaltung beinhalten. Diese sollte individuell auf die Bedürfnisse der Organisation zugeschnitten sein. Jedes Unternehmen verfügt über andere digitale Anlagen. Dazu gehören Smartphones oder Laptops, verschiedene Anwendungen oder Software-as-a-Service (SaaS). Früher konnten IT-Manager digitale Anlagewerte mit einer Tabellenkalkulation verwalten. Solche Standardansätze eignen sich jedoch nicht für das dynamische digitale Umfeld von heute: ein Umfeld, das auch die Nutzung von Cloud-Infrastrukturen und Open-Source-Anwendungen umfasst und in dem Organisationen ernsthaften Bedrohungen wie Ransomware-Angriffen oder Cyberdiebstahl ausgesetzt sind.

Unternehmen können ihre digitalen Anlagewerte auf unterschiedliche Weise verwalten, etwa mithilfe von Bestandslisten in der Cloud, Software zur Erkennung von Sicherheitslücken oder Konfigurationsmanagement-Software. Bei kleineren Firmen geschieht das vielleicht manuell – besonders bei physischen Anlagewerten wie Servern und Netzwerkgeräten. Doch die digitale Belegschaft von heute ist auf mehrere Endgeräte angewiesen. Sie alle muss das Unternehmen schützen. Nur wenn Unternehmen ihre digitalen Bestände und deren Schwachstellen kennen, können sie Risiken genau einschätzen und die erforderlichen Sicherheitsmaßnahmen ergreifen.

Unternehmen brauchen ein automatisiertes Patch-Management-Protokoll.

Ohne ein strenges Patch-Protokoll können Systeme veralten und für Tage oder sogar Wochen angreifbar sein – das öffnet einer möglichen Katastrophe Tür und Tor. Auch bereits installierte Patches können Schwachstellen aufweisen. IT-Verantwortliche wissen, dass böswillige Hacker solche Sicherheitslücken ausnutzen, doch die meisten Unternehmen können sich nur mit einer von zehn neuen Schwachstellen pro Monat beschäftigen. Viele Unternehmen sind nicht in der Lage, Schwachstellen zu beseitigen, sobald sie entdeckt werden – auch wenn Cyberexperten betonen, wie wichtig das ist.

> *„Trotz des ganzen Branchenrummels um die neueste Zero-Day-Lücke haben es böswillige Akteure regelmäßig auf alte Schwachstellen abgesehen.“*

Ein effektives Patch-Management-System errichtet eine Verantwortungspyramide. Ihr gehören Mitarbeitende an, die für Wartung und Fehlerbehebung zuständig sind, Führungskräfte, die Abläufe festlegen und

regelmäßige Bestandsaufnahmen machen, sowie IT-Mitarbeitende, die sich um Anwendungen, die Cloud, mobile Geräte und andere Plattformen kümmern.

Ihr Unternehmen kann Patching natürlich manuell durchführen. Eine automatisierte Fehlerbehebung ist jedoch effizienter, weil sie nicht die Zeit und Aufmerksamkeit von Fachleuten beansprucht. Automatisierte Systeme schließen Sicherheitslücken, sobald sie auftreten. Dadurch stehen alle digitalen Funktionen weiter in vollem Umfang zur Verfügung, was sowohl für Ihre Mitarbeitenden als auch für Ihre Kundschaft von Vorteil ist. Allerdings kann die Automatisierung erfordern, dass Sie Mitarbeitende im Patch-Management schulen. Zudem werden manche Schwachstellen möglicherweise noch nicht von vorhandenen Patches abgedeckt.

Einzelpersonen und Unternehmen sollten Systeme zur digitalen Regulierung einrichten.

Einige Sicherheitslücken handeln Sie sich unweigerlich mit Software und in der Cloud verfügbaren Diensten ein. Andere entstehen durch die spezifischen Konfigurationen bestimmter Softwareprodukte. Unternehmen müssen daher professionell konzipierte Richtlinien verabschieden, um die bestmöglichen Sicherheitsmaßnahmen zu etablieren. Beispiele finden Sie beim Center for Internet Security (CIS) oder dem Cybersecurity Framework (CSF) des National Institute of Standards and Technology (NIST).

> *„Während die Schlagzeilen im Bereich Cybersicherheit oft von der neuesten Zero-Day-Schwachstelle dominiert werden, sind viele bedeutende Datenschutzverletzungen in Wahrheit auf Fehlkonfigurationen zurückzuführen.“*

Fehlkonfigurationen sind Fehler oder Unzulänglichkeiten innerhalb eines Informationssystems, die Sicherheitslücken zur Folge haben können. Für Fehlkonfigurationen gibt es mehrere Ursachen. Zum Beispiel können Softwareanwendungen unsichere Standardeinstellungen aufweisen. Darüber hinaus kontrollieren einige Dienste den Zugang zu gefährdeten Einstellungen nicht ausreichend. Obwohl Unternehmen sich der Risiken bewusst sind, gewähren viele von ihnen zu vielen Mitarbeitenden unnötige Zugriffsrechte. Womöglich überwachen sie auch ihr Netzwerk nicht sorgfältig genug und sind nicht in der Lage, schnell auf Sicherheitsvorfälle oder Fehlkonfigurationen zu reagieren. Oder es fehlt an einer wirksamen Patch-Management-Strategie.

Schwachstellenmanagement erfordert höchste Wachsamkeit und kontinuierliche Überwachung.

Schwachstellenmanagement dürfen Sie nicht nur hin und wieder betreiben. Sie müssen sich fortlaufend und dauerhaft damit beschäftigen, da Anlagen und Konfigurationen sich mit der Zeit ändern. Neue Mitarbeitende treten ins Unternehmen ein, andere wechseln die Stelle innerhalb der Firma. Wenn dies geschieht, sollten Sie die internen Privilegien und Berechtigungen entsprechend anpassen. In einer dynamischen, sich schnell verändernden Arbeitsumgebung entstehen ständig neue Sicherheitslücken.

Kontinuierliches Schwachstellenmanagement umfasst eine Reihe von Schritten. Zunächst – und das ist ein Schritt, den viele Unternehmen versäumen – sollten Sie einen Prozess aufsetzen, mit dessen Hilfe Sie Schwachstellen ermitteln. Legen Sie fest, was Ihr Unternehmen tun wird, wenn Probleme auftauchen.

Überwachen und dokumentieren Sie, wie Ihr Team damit umgeht. So sehen Sie, wie gut Sie auftretende Probleme lösen.

Da Schwachstellen im Lauf der Zeit exponentiell zunehmen, müssen Unternehmen das Patch-Management automatisieren und interne wie externe Anlagen in regelmäßigen Abständen automatisch auf Sicherheitslücken untersuchen.

Weisen Sie Schwachstellen bestimmte Werte zu, damit Sie sie priorisieren können.

Wenn Sie Schwachstellen objektiv bewerten, ermöglicht das Ihren Mitarbeitenden, den potenziellen Schaden zu begrenzen. Eine Schwachstellenrangordnung hilft, zu entscheiden, welche Sicherheitslücken oder etwaigen Datenschutzverstöße Priorität haben. Die meisten Unternehmen verwenden das Common Vulnerability Scoring System (CVSS), das das Forum of Incident Response and Security Teams (FIRST) 2005 eingeführt hat.

> *„Im Kern besteht das Ziel des CVSS darin, eine numerische Punktzahl auszugeben, die den Schweregrad einer Schwachstelle im breiten Spektrum bekannter Schwachstellen angibt.“*

Das Programm wurde seit seiner Einführung mehrfach aktualisiert. Die aktuelle Version ist CVSS 4.0. Es unterteilt Schwachstellen in folgende vier Kategorien:

1. **Basis** – Dieser Wert spiegelt die spezifischen Eigenschaften der betreffenden digitalen Umgebung wider und ändert sich nicht.
2. **Bedrohung** – Hier werden verschiedene Gefahren und deren Ausmaß eingeschätzt.
3. **Umwelt** – Hier werden die Schwachstellen aufgeführt, die sich aus der digitalen Umgebung und ihrer Struktur ergeben.
4. **Ergänzung** – Hier werden menschliche Faktoren ergänzt, etwa wie dringlich eine Schwachstelle ist und ob sie ein Sicherheitsrisiko für die Nutzerinnen und Nutzer mit sich bringt.

Für sich genommen kann das CVSS Probleme nicht mit absoluter Genauigkeit priorisieren. Das Exploit Prediction Scoring System (EPSS) erweitert das CVSS: Es liefert Information zur Wahrscheinlichkeit, mit der ein Cyberkrimineller an einer bestimmten Sicherheitslücke ansetzen wird. Tatsächlich werden nur 2 bis 7 Prozent der meisten Schwachstellen tatsächlich ausgenutzt.

Cyberangreifer nutzen zahlreiche Schwachstellen aus.

Cyberkriminelle können bei älteren Schwachstellen ansetzen, um einen Cyberangriff zu starten. Wenn Ihr Unternehmen ältere Software in neuen Infrastrukturen und Technologien einsetzt, können dadurch Sicherheitslücken entstehen. Mehr als die Hälfte der Sicherheitslücken in Unternehmen stammt aus dem Jahr 2016 oder früher.

> *„Es ist durchaus möglich, dass Angreifer ältere Sicherheitslücken ausnutzen, um Verkettungsangriffe auf kritische Schwachstellen durchzuführen.“*

Bei Verkettungsangriffen führt eine Schwachstelle zur nächsten. Die Verkettung kann direkt oder indirekt sein. Eine direkte Verkettungsattacke könnte zum Beispiel damit beginnen, dass der Authentifizierungsprozess eines Systems umgangen wird. Ein indirekter Verkettungsangriff könnte mit einem gestohlenen Passwort seinen Anfang nehmen. Jeder Ansatzpunkt eröffnet mehrere Angriffsmöglichkeiten. Angreifer bewegen sich in einem attackierten System von Anwendung zu Anwendung und nutzen Schwachstellen aus, sobald sie auftauchen.

Mithilfe von öffentlich zugänglichen Informationen können Sie herausfinden, welchen Bedrohungen Sie ausgesetzt sind.

Fachleute für Cybersicherheit nutzen Open-Source-Informationen, um das Ausmaß der Bedrohung für eine Organisation einzuschätzen. Threat-Intelligence-Teams untersuchen, ob ein System häufig bestimmte IP-Adressen, Dateitypen oder Schwachstellen aufweist. Anschließend verwenden sie diese Informationen, um Warnungen zu erstellen, Angriffe zu identifizieren und zu blockieren und bei der Wiederherstellung zu helfen.

> *„Es ist wichtig, die verschiedenen Bedrohungsdaten zu verstehen, die das Schwachstellenmanagement nutzt.“*

Es gibt vier Arten von Bedrohungsdaten, die Sie im Blick haben müssen:

1. Bei „technischen Bedrohungsdaten“ geht man davon aus, dass ein Angriff stattgefunden hat und dass die Verteidiger die Spuren des Angriffs nutzen können, um den Täter zu finden.
2. Um „taktische Bedrohungsdaten“zu erhalten, untersucht man die Methoden, die ein böswilliger Akteur für einen Angriff verwenden könnte, darunter Malware, Ransomware, Phishing und verschiedene Arten von Netzwerk-Scans.
3. „Strategische Bedrohungsdaten“ sind Informationen für Führungskräfte und politische Entscheidungsträger. Diese Daten umfassen nationale und internationale Vorschriften. Man sammelt sie aber auch in regionalen, nationalen und internationalen Medien sowie in den sozialen Medien.
4. „Operative Bedrohungsdaten“ gewinnt man, indem man Daten zu den Anreizen, Motiven und Methoden böswilliger Akteure zusammenträgt.

Ein Threat-Intelligence-Programm entbindet Sie nicht davon, ein Schwachstellenmanagement aufzusetzen und zu pflegen. Sobald dieses ausgereift ist, können Unternehmen es durch die Einführung von Threat Intelligence verbessern. Dies hilft Einzelpersonen und Unternehmen, die Kaskade von Sicherheitslücken zu sortieren und zu organisieren und sich auf die Lösung von Problemen zu konzentrieren.

Die Mitwirkung von Menschen ist im Schwachstellenmanagement entscheidend.

Auch wenn wir in einer Welt der Spitzentechnologie und der Cybersicherheit leben, kommt es letztlich doch immer auf den Menschen und seine psychologische Verfassung an. Ja, Ihr Unternehmen braucht ein Schwachstellenmanagement, das viele verschiedene Tools, Systeme und Faktoren nutzt – aber Ihre Mitarbeitenden werden es verwalten, nicht Ihre Maschinen.

„Organisationen können ein besseres Schwachstellenmanagement entwickeln, wenn sie verstehen, wie sowohl ihre Nutzer als auch die IT- und Sicherheitsfachleute mit den Systemen interagieren.“

„Human factors engineering“ berücksichtigt menschliche Fähigkeiten und Grenzen bei der Entwicklung von Tools und anderen Produkten, einschließlich digitaler Systeme. Digitale Tools interagieren mit ihren Nutzerinnen und Nutzern, weshalb zunehmend Designprinzipien angewendet werden, die Aspekte der menschlichen Denkweise einbeziehen. Das „Human factor security engineering“ beachtet psychologische Faktoren bei der Ausbildung von Cybersicherheitsexperten.

Cyberangriffe nehmen ständig zu. Da dabei vermehrt künstliche Intelligenz zum Einsatz kommt, werden die Angriffe immer ausgefeilter. Cybersicherheitsexperten sollten in ihrer Ausbildung Kenntnisse über die menschliche Psychologie erwerben. Dadurch erhalten sie Einblick in die Denkweise von Cyberkriminellen. Dieses Wissen kann ihnen aber auch dabei helfen, ihre eigenen Arbeitspläne so zu gestalten, dass sie Erschöpfung und Burn-out vorbeugen, die bei IT- und Cybersicherheitspersonal weitverbreitet sind.

Führungskräfte sollten beim Aufbau ihrer Organisation die Sicherheit im Blick haben.

In puncto Cybersicherheit müssen Organisationen mit Sicherheitslücken und Bedrohungen zurechtkommen, doch es braucht auch einen Mentalitätswandel. Software sollte von vornherein sicher sein. Bereits bei der Entwicklung von Software und Systemen muss der Aspekt der Sicherheit berücksichtigt werden.

Unternehmen können sich heute vor Sicherheitslücken kaum retten. Ein Problem ist, dass Entwicklerinnen und Entwickler dazu neigen, Software und digitale Systeme zu entwerfen, ohne schon in der Entwicklungsphase Sicherheitsaspekte einzubeziehen. Die zunehmende Nachfrage nach sicheren Produkten wird diesen Ansatz jedoch verändern und sich auf die Marktdynamik auswirken. Sie wird Anbieter zwingen, digitale Produkte zu entwickeln, die Nutzerinnen und Nutzer vor böswilligen Cyberakteuren schützen.

Die Hersteller müssen Verantwortung für die Sicherheit ihrer Produkte übernehmen. Sie müssen Digitalprodukte auf den Markt bringen, die von vornherein sicher sind und die Nutzerinnen und Nutzer nicht zwingen, zusätzliche Sicherheitsmaßnahmen zu ergreifen. Zugleich muss die Kundschaft jedoch auf Transparenz und Verantwortung bestehen und ihre Unternehmen so führen, dass die Belegschaft die Sicherheitsziele unterstützt und fördert.

Über die Autoren

Chris Hughes ist außerordentlicher Professor für Cybersicherheit an der Capitol Technology University sowie der University of Maryland Global Campus. Außerdem ist er Mitgründer und Präsident von Aquia. **Nikki Robinson** gibt Graduiertenkurse an der Capitol Technology University und am Touro College.