RAPID7

WHITEPAPER

Best Practices der Cybersecurity

für sichere Netze und Anwendungen

Mit Rapid7 sicher vorankommen

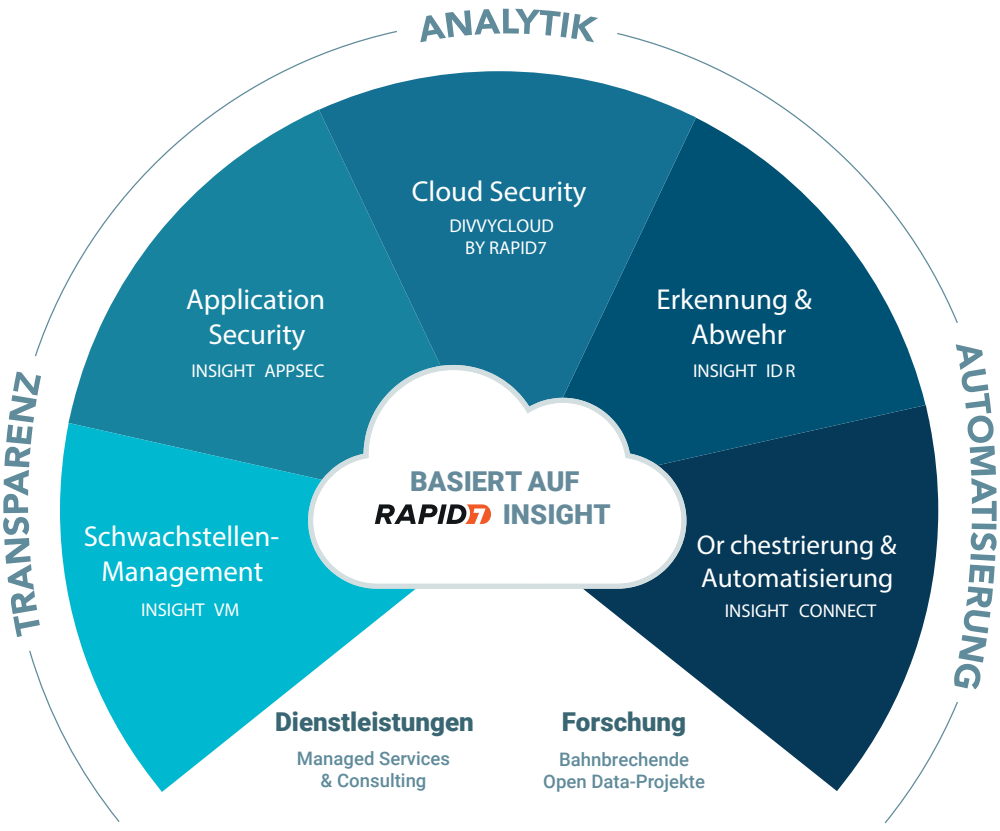
Das Jahr 2020 hat vieles verändert, darunter auch die die Art und Weise, wie wir über IT-Sicherheit denken und Risiken priorisieren.

Damit Sie und Ihr Team konzentriert und energisch daran arbeiten können, Ihre Organisation sicher voranzubringen, haben wir für Sie diesen Leitfaden zusammengestellt.

Zudem haben wir eine Serie von drei Webinaren zu den behandelten Themen abgehalten, die Sie sich hier ansehen können:

https://events.rapid7.com/cybersecurity-best-practices-webcast-series

Organisationen rund um die Welt bauen auf die Technologien, die Dienstleistungen und die Forschung von Rapid7, um ihre Unternehmen sicher voranzubringen. Unsere Insight-Cloud setzt auf Transparenz, Analyse und Automatisierung. Das vereinfacht komplexe Sachverhalte und unterstützt Sicherheitsteams dabei, Vulnerabilities zu beheben, schädliche Aktivitäten zu erkennen, Angriffe zu untersuchen und abzuwehren sowie Abläufe zu automatisieren.



TEIL 1

Vier Strategien für eine schnelle und sichere Migration in die Cloud

In der ersten Hälfte des Jahres 2020 hat die Nutzung der Cloud als Reaktion auf die Auswirkungen der Pandemie erheblich zugenommen. 51%[1] der Unternehmen planen, mehr Anwendungen in die Cloud zu verlagern, um sich auf künftige Shutdowns vorzubereiten.

Figure 1: Of enterprises are planning to move more applications to the cloud to prepare for future shutdowns.

Dennoch wäre es verkehrt zu glauben, dass die Ereignisse des Jahres 2020 der Hauptgrund für die Einführung der Cloud waren. Der Druck zur Innovation und zur Steigerung der Wettbewerbsfähigkeit ist nach wie vor die Haupttriebkraft für die Cloud, und die Unternehmen sind bereit. Eine Studie[2] von DivvyCloud (jetzt Teil der Rapid7-Familie) ergab, dass eine Mehrheit der Befragten sich in der letzten Phase ihrer Cloud Journey befindet. 59% gaben an, dass sie sich in der DevOps-Optimierungsphase befinden (ein Anstieg von 11% im Vergleich zum letzten Jahr), und 36% gaben an, dass sie derzeit ihre Cloud Operations optimieren.

Bei der zunehmenden Cloud-Adoption gibt es jedoch in vielen Fällen eine klaffende Lücke: Von den Unternehmen, die bereits die öffentliche Cloud nutzen (93%), bestätigten nur 40%[3], dass sie über einen Ansatz zur Verwaltung der Cloud- und Containersicherheit verfügen. In der agilen Entwicklungswelt, in der wir heute leben, wird Sicherheit oft als die Handbremse der Innovation angesehen.

Laut Gartner[4] werden im Jahr 2023 99% der Sicherheitsmängel in der Cloud auf die Schuld des Kunden zurückzuführen sein. Und "bis zum Jahr 2024 werden Organisationen, die ein Cloud Security Posture Management (CSPM) implementieren und dieses in die Entwicklung einbeziehen, cloud-bezogene Sicherheitsvorfälle aufgrund von Fehlkonfigurationen um 80% reduzieren".

Die obige Prognose wird erhebliche Konsequenzen haben. Allein in den Jahren 2018 und 2019 kosteten Fehlkonfigurationen[5] der Cloud die Unternehmen schätzungsweise 5 Billionen Dollar. Und in einer Krise wird es nur noch schlimmer. Bedrohungsakteure gehen davon aus, dass potentielle Opfer besorgt und gestresst und daher weniger abwehrbereit sind. Dadurch erhöht sich die Chance, Schaden anzurichten und finanziellen Gewinn zu erzielen. Wie wir in den letzten sechs Monaten gesehen haben, nehmen Cyber-Angriffe zu, insbesondere bei Organisationen und Institutionen im Gesundheitswesen, die bereits unter dem Stress der Pandemie stehen.

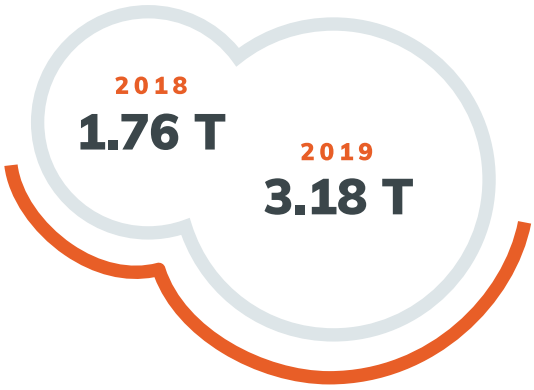


Figure 2: Cloud misconfigurations cost enterprises an estimated $5 Trillion in 2018 and 2019 alone.

Die Wahl zwischen Innovation und Sicherheit

Offensichtlich haben Entwickler das Gefühl, dass Sicherheits- und Konformitätsrichtlinien sie bei der schnellen und effizienten Entwicklung und Implementierung neuer Dienste behindern. Viele wählen die einfache Antwort und entscheiden sich dafür, solche Richtlinien zu umgehen. Laut der DivvyCloud-Umfrage[6] gibt es eine Kultur des Vermeidens, um Dinge schnell zu erledigen.

- **Von den Befragten, die bestätigten, dass ihre Organisation die öffentliche Cloud nutzt, verfügen nur etwas mehr als die Hälfte (58%) über klare Richtlinien für Entwickler, die Anwendungen erstellen und in der öffentlichen Cloud arbeiten.**
- **Und von diesen gaben 25% an, dass diese Richtlinien nicht durchgesetzt werden, während 17% bestätigten, dass es ihrer Organisation völlig an klaren Richtlinien mangelt.**
- Zu allem Überfluss gab fast die Hälfte (49%) aller Befragten, die öffentliche Clouds nutzen, an, dass ihre Entwickler und Ingenieure manchmal die Sicherheits- und Konformitätsrichtlinien der Cloud ignorieren oder umgehen.

Offensichtlich sind viele der Meinung, dass sie sich zwischen Sicherheit und Innovation entscheiden müssen. Es ist Zeit für einen neuen Ansatz und eine neue Denkweise.

1 MariaDB, COVID-19's Impact on Cloud Adoption
2 2020 State of Enterprise Cloud Adoption and Security
3 2020 State of Enterprise Cloud Adoption and Security
4 Neil MacDonald, "Innovation Insight for Cloud Security Posture Management", Gartner.com, January 25, 2019
5 2020 Cloud Misconfigurations Report
6 2020 State of Enterprise Cloud Adoption and Security

STRATEGIE

01 | Konvergenz ist der Schlüssel

Immer wieder hören wir in der IT-Welt den Begriff “Alignment”. Das bedeutet, dass Business und IT aufeinander abgestimmt werden müssen, bzw. in diesem Fall, dass Sicherheitsteams (SecOps) und Entwicklungsteams (DevOps). Aber ist das genug? Das Sicherheitsteam kann sich zum Beispiel hinsichtlich seiner Ergebnisse oder Ziele mit dem Entwicklungsteam “abstimmen”, behält aber dennoch seinen Status als eigenständiges Team.

Konvergenz geht weiter. Sie erfordert die tatsächliche Zusammenlegung von Teams auf einer dauerhafteren Basis, so dass wirklich ein Team mit gemeinsamen KPIs entsteht. Doch sehr oft erweist sich der Unterschied in der Denkweise als eines der größten Hindernisse für SecOps, mit Planungs-, Entwicklungs- und Operations-Teams an einem Tisch zu sitzen. Die Arbeitsweisen sind zu unterschiedlich. Doch der Wunsch nach Agilität, Schnelligkeit auf dem Markt und Größe muss mit Sicherheit, Risiko und Compliance in Einklang gebracht werden.

Die Offenheit für Veränderungen und neue Ideen wird dem gesamten Entwicklungsprozess erheblichen Mehrwert verleihen. Doch welche praktischen Schritte kann man unternehmen, um diesen kulturellen Wandel voranzutreiben?

Managementkette - Wenn beide Rollen durch die gleiche(n) Person(en) nach oben berichten, gewährleistet dies einen einheitlichen Ansatz und ein einheitliches Verständnis.

Gemeinsame KPIs - Obwohl jede Rolle einen anderen Schwerpunkt hat, kann ein Projekt nur dann erfolgreich durchgeführt werden, wenn gemeinsame KPIs exisitieren, was bedeutet, dass beide Rollen die gleichen Instrumente und den gleichen Ansatz verwenden müssen.

Reduzieren Sie den Technologie-Stack - Die meisten Unternehmen haben eine Vielzahl unterschiedlicher Sicherheitspakete. Eine Reduzierung der Komplexität kann die Dinge für Entwickler erheblich vereinfachen.

STRATEGIE

02 | Geschwindigkeit und Sicherheit im Gleichgewicht

Cloud-Governance wird oft als separate Einheit behandelt, wobei viele Organisationen davon ausgehen, dass der Cloud-Anbieter ihre sensiblen Informationen schützt. Diese Denkweise geht zurück auf die Zeit, als Server vor Ort und interne Cloud-Umgebungen die Norm waren, wobei die IT lediglich den Geschäftsbetrieb ergänzte.

Doch da die Cloud heute ein wesentlicher Bestandteil des Geschäftsbetriebs ist, ist es unerlässlich, die Cloud-Governance in die allgemeine Risiko-Governance des Unternehmens einzubinden. Erst dann konzentriert das Unternehmen seine gesamten Ressourcen darauf, seine in der Cloud gehosteten Daten und Anwendungen vor unbefugtem Zugriff zu schützen.

Darüber hinaus ist es beim Umstieg auf oder bei der Entwicklung von Cloud-basierten Anwendungen sehr wichtig, Sicherheitslücken so früh wie möglich zu erkennen und einen Aktionsplan zur Behebung zu entwickeln, bevor die Anwendung in Produktion geht. Eine Möglichkeit besteht darin, Ihr Entwicklungsteam in die Lage zu versetzen, die Abhilfe selbst in die Hand zu nehmen und das Problem als ihres zu akzeptieren.

Ein Lehrplan für Sicherheits-Trainings, in denen Entwickler darin geschult werden, Schwachstellen zu erkennen und zu beheben, ist ein guter Anfang. Die drei häufigsten Schwachstellen von Webanwendungen sind zum Beispiel:

- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)

Verständlicherweise ist eine Verhaltensänderung jedoch eine Herausforderung, egal um welche Rolle es sich handelt. Wer außerhalb seiner gewohnten Handlungsweisen oder Prozesse agieren muss, ist unter Umständen weniger geneigt, sich zu beteiligen, wodurch größere Reibungen zwischen den beiden Teams entstehen können. Daher ist die Verlagerung der Cloud-Sicherheit in den Prozess der kontinuierlichen Integration und Bereitstellung (Continuous Integration, Continuous Delivery, CICD) eine weitere großartige Strategie, die man verfolgen sollte. Strategie vier (unten), die sich mit der Automatisierung befasst, führt dies weiter aus.

STRATEGIE

03 | Auf Risiken statt auf Bedrohungen konzentrieren

Cybersicherheit ist nur so effektiv wie ihre Governance. Genauso wichtig ist eine unabhängige Aufsicht über die Sicherheitsrisiken durch einen Chief Risk Officer oder eine andere unabhängige Instanz. Diese Rolle kontrolliert den CISO oder den IT-Sicherheitsbeauftragten sowie den Cloud-Anbieter. Diese wichtige Verteidigungslinie bietet eine unabhängige Aufsicht, die gegebenenfalls bei der Identifizierung, Eindämmung, Eskalation und Behebung von Risiken hilft.

Die Verlagerung von Workloads in die Cloud birgt jedoch neue Risiken für Organisationen. In der Regel bieten öffentliche Clouds einen grundlegenden Schutz, der sich jedoch hauptsächlich auf die Sicherung der Infrastruktur konzentriert. Dadurch können Workloads anfällig werden. Aus diesem Grund besteht in bereitgestellten Cloud-Umgebungen nicht nur die Gefahr von Account-Kompromittierung und Datenverlusten, sondern auch die Gefahr der Ressourcenausbeutung aufgrund von Fehlkonfigurationen, mangelnder Visibility oder Benutzerfehlern.

Die meisten Angriffe lassen sich verhindern, indem Software-Schwachstellen und Cloud-Fehlkonfigurationen behoben werden sowie Strategien und Best Practices für das Identity Management in der Cloud eingesetzt werden. Hier eine Checkliste zur Sicherheit in der Cloud:

- Identifizieren Sie öffentlich exponierte Assets (achten Sie besonders auf Speicher-, Datenbank-, Such- und Cache-Dienste)
- Identifizieren und entfernen Sie übermäßige und ungenutzte Berechtigungen
- Härten Sie Sicherheitskonfigurationen
- Sichern Sie APIs
- Decken Sie versuchte Datendiebstähle oder Sicherheitsvorfälle auf
- Automatisieren Sie Cloud-Sicherheitsfunktionen

STRATEGIE

04 | Beschleunigung durch Orchestrierung und Automatisierung

Die Komplexität und das wachsende Risiko von Cloud-Umgebungen übertragen auch den Entwicklern mehr Verantwortung für das Schreiben und Testen sicherer Anwendungen. Die meisten sind zwar keine Cloud-orientierten Sicherheitsexperten, aber es gibt viele Dinge, die wir tun können, um zu helfen (einschließlich einer besseren Ausbildung, wie bereits erwähnt) und zu einer verbesserten Sicherheitshaltung beizutragen.

Die Verwendung von Pipelines und Infrastructure-as-Code (IaC) sind wichtig, um die Cloud-Sicherheit in CICD zu überführen. Auf diese Weise wird sichergestellt, dass Entwickler sich mit größerer Wahrscheinlichkeit beteiligen, was zu weitaus besseren Sicherheitsergebnissen führt. Allerdings können sich bei der Nutzung von IaC-Tools, z.B. Terraform oder cft, als Teil des CICD-Cloud-Prozesses in IaC-Templates enthaltene Fehler in der Cloud-Konfiguration schnell ausbreiten und enorme Sicherheitslücken aufreißen. Solche Probleme während des CICD-Prozesses zu lösen ist weitaus besser als zur Laufzeit, wo kurzlebige Ressourcen einfach durch den nächsten Build ersetzt werden.

Die Vorteile der Automatisierung sind zahlreich:

- Zeit wird dadurch gespart, dass die Menschen nicht mehr manuell reagieren und handeln müssen. Die Aktionen werden automatisch ausgeführt, so dass die Mitarbeiter an Aufgaben mit höherer Wertschöpfung arbeiten können.
- Verbesserte Sicherheit resultiert daraus, dass Schwachstellen sofort nach ihrer Entdeckung behoben werden, wodurch verhindert wird, dass Angreifer Probleme ausnutzen.
- Jede Aktion folgt einem genau definierten Workflow. Organisationen können sicher sein, dass die vorgeschriebenen Verfahren stets korrekt und konsistent befolgt werden.
- Statt durch regelmäßige Audits können Sie die Konformität durch eine kontinuierliche Protokollierung und den Nachweis von Korrekturen in Echtzeit aufrechterhalten und nachweisen.

Die Automatisierung reicht von der einfachen Benachrichtigung und Protokollierung bis hin zur fortschrittlichsten Art, der vollautomatischen Korrektur. Sie müssen jedoch nicht vom ersten Tag an mit einer 100%ig automatisierten Korrektur beginnen. Tatsächlich profitieren die meisten Unternehmen davon, sich durch die Automatisierungsstufen zu arbeiten, um vollständig zu erkunden, welche Ansätze am besten zu ihrer Umgebung passen. Mehr über die verschiedenen Schritte und Automatisierungsebenen erfahren Sie in diesem ausgezeichneten Papier von Divvy Cloud, das die vier Automatisierungsebenen behandelt.

Wählen Sie nicht, sondern führen Sie zusammen

Auch wenn es oft verlockend ist, die Sicherheit zugunsten eines raschen Deployments zu umgehen, können die Folgen für Ihre Organisation im weiteren Verlauf verheerend sein, wenn es Angreifern gelingt, sich durch Schwachstellen zu schleichen. Und wenngleich die SecOps- und die DevOps-Teams die Dinge sehr unterschiedlich angehen, können beide Teams voneinander lernen, um sicherzustellen, dass Organisationen nicht nur großartige Produkte und Lösungen hervorbringen, sondern dass diese auch in hohem Maße sicher sind.

Auch wenn es oft verlockend ist, die Sicherheit zugunsten eines raschen Deployments zu umgehen, können die Folgen für Ihre Organisation im weiteren Verlauf verheerend sein

https://www.rapid7.com/

TEIL 2

Anwendungssicherheit - Wer breiter testet, testet besser

Die explosionsartige Zunahme der Apps in den letzten Jahren ist geradezu phänomenal. Nach der Untersuchung von fast 5 Millionen Stunden Live-Desktop-Aktivität der Mitarbeiter des operativen Supports ergab ein Bericht von Pegasystems Inc., dass der durchschnittliche Mitarbeiter täglich mehr als 1.100 Mal zwischen 35 jobrelevanten Anwendungen wechselt. Und man kann mit Fug und Recht behaupten, dass die Cloud-Infrastruktur dies möglich gemacht hat. Sie hat unser gesamtes Denken und die Kultur unserer Arbeitsweise verändert.

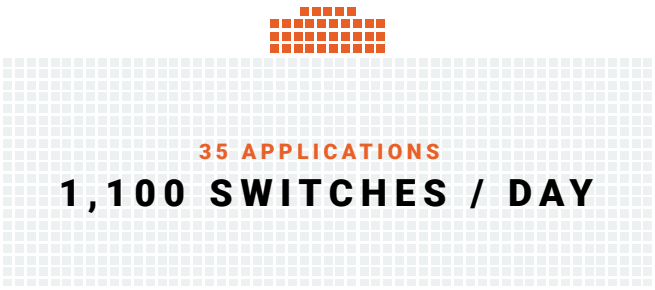


Figure 3: The average employee switches between 35 applications more than 1,100 times every day.

Wenn wir die vergangenen Zeiten betrachten, so erforderte die Erledigung jeder Art von arbeitsbezogenen Aufgaben einen Besuch im Büro oder zumindest den Einsatz eines PCs oder mobilen Geräts mit dem richtigen VPN-Client, der darauf installiert war. Heutzutage können die Mitarbeiter auf alles, was sie zur Ausübung ihrer Tätigkeit benötigen, von so ziemlich jedem Ort aus über jedes Gerät mit einer einfachen Internetverbindung zugreifen. Von der Erstellung von Spesenabrechnungen über das Ausfüllen von Stundenzetteln und die Überprüfung von Lagerbeständen bis hin zur Möglichkeit, eine Vielzahl anderer wichtiger Funktionen zu verwalten, die den Geschäftsbetrieb aufrecht erhalten.

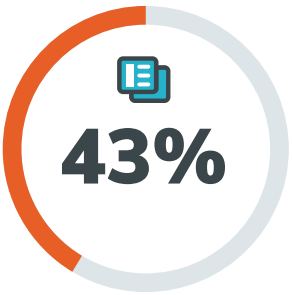


Figure 4: 43% of breaches were attacks on web applications

Und während viele Organisationen mit ihrer "Cloud-Reise" gut unterwegs sind, haben die Ereignisse der ersten Hälfte des Jahres 2020 (und wahrscheinlich auch darüber hinaus) die Dinge noch weiter beschleunigt und die Zögerlichen zum Handeln gezwungen. Die durch die globale Pandemie bedingte Auslagerung der Mitarbeiter hat zu einer noch größeren Nachfrage nach dem Zugang zu Geschäftsanwendungen geführt. Die meisten Organisationen mussten innerhalb weniger Tage einen Plan für die Heimarbeit entwickeln und umsetzen. Vorteilhaft war dabei, dass z.B. Webanwendungen hervorragend zu der neuen Betriebsumgebung passten, in der wir uns befinden. Sie sind von Natur aus plattformübergreifend, wodurch die Notwendigkeit entfällt, für jede Benutzerplattform separate Anwendungen zu entwickeln.

Applikationen werden häufig angegriffen

Doch gerade während einer Krise, wenn die Gedanken am meisten abgelenkt sind, wird das Risiko von Bedrohungen noch offensichtlicher. Und die Anwendungen scheinen das große Ziel von Angreifern zu sein. Sie sind der primäre Angriffsvektor bei Sicherheitsverletzungen: Weltweit gaben 42%[7] der Entscheidungsträger im Bereich der Sicherheit, deren Firmen einen Angriff von außen erlebten, an, dass dieser unter Ausnutzung einer Software-Schwachstelle durchgeführt wurde. Fünfunddreißig Prozent gaben an, dass der Angriff über eine Webanwendung erfolgte.

Und das ist noch nicht alles. Ein Bericht von Verizon[8] legt nahe, dass 43% der Verstöße Angriffe auf Webanwendungen waren, mehr als doppelt so viele wie im Vorjahr. Die Bedrohung ist sehr real:

- **Geschäftskritische Daten landen in der Öffentlichkeit: Das heißt, Anwendungen enthalten geschäftskritische Daten und machen sie über das Internet zugänglich.**
- **Exploits nutzen die Funktionalität der Anwendung: Viele Exploits nutzen die beabsichtigte Funktionalität der Anwendung aus, so dass es sehr schwierig ist, Abhilfe zu schaffen, ohne diese Funktionalität einzuschränken.**
- **Ausfallzeiten sind extrem teuer: Die Verfügbarkeit der Anwendung ist absolut entscheidend. Viele Unternehmen führen ihre Kernprozesse über Anwendungen aus; jede Ausfallzeit kann Umsatzeinbußen bedeuten, die sich auf die Performance des Unternehmens und letztlich auf den Gewinn auswirken.**
- **Die Wiederherstellung kann Jahre dauern: Ein einziger Verstoß kann die Marke erheblich schädigen und einen CISO letztlich den Job kosten.**

Läufer, Radfahrer und Luftfahrtexperten werden kürzlich mitbekommen haben, wie der Hersteller von Smartwatches und Wearables, Garmin, Opfer eines Lösegeldangriffs auf seine Dienste und Anwendungen wurde. Der Angriff veranlasste Garmin dazu, seine offizielle Website, den Benutzerdaten-Synchronisierungsdienst Garmin Connect, die Datenbankdienste von Garmin für die Luftfahrt und sogar einige Produktionslinien in Asien zu schließen. Während das Potenzial für Daten- und Umsatzverluste für Garmin enorm war, scheinen die Nutzer des Dienstes eher besorgt darüber zu sein, dass sie ihre letzten Aufzeichnungen nicht hochladen können. Und das ist kritisch! So werden sie unweigerlich zum nächsten Wettbewerber gehen, laufen, fahren oder fliegen.

Wenn also Anwendungen den Organisationen in einer postpandemischen Welt Kopfschmerzen bereiten, wie kann man sie am besten schützen und die Geschäftskontinuität gewährleisten? Zunächst betrachten wir einen sicheren Software Development Lifecycle (SDLC), der beschreibt, wie Software-Teams sichere Anwendungen erstellen.

7 Forrester, May 2020
8 Verizon Data Breach Investigations Report, 2020

Eine Landschaft im Wandel

Traditionell haben die Sicherheitsteams Tests durchgeführt, die sich in der Regel auf die Erfüllung von Konformitätsstandards konzentrierten. Es handelt sich um einen sicherheitszentrierten Ansatz, bei dem der Schwerpunkt auf Risiko und Belastbarkeit liegt, sowohl intern als auch extern. Geschwindigkeit und Effizienz leiden jedoch darunter.

Das Konzept des "Shift Left" ist seit einiger Zeit ein beliebter Trend in der kontinuierlichen Testpraxis. Das heißt, das Testen zu einem früheren Zeitpunkt im SDLC, um Fehler billiger beheben zu können und das Risiko der Einführung neuer Angriffsvektoren zu verringern. Und obwohl dies logischerweise ein vernünftiger Ansatz zu sein scheint (und immer noch sehr wichtig ist), zeichnen sich jetzt auch Shift Right-Praktiken beim Testen als Trend ab. Auf diese Weise können sich Teams vor Problemen und Angreifern schützen, die nicht auf bekannte Exploits oder Probleme im Code setzen.

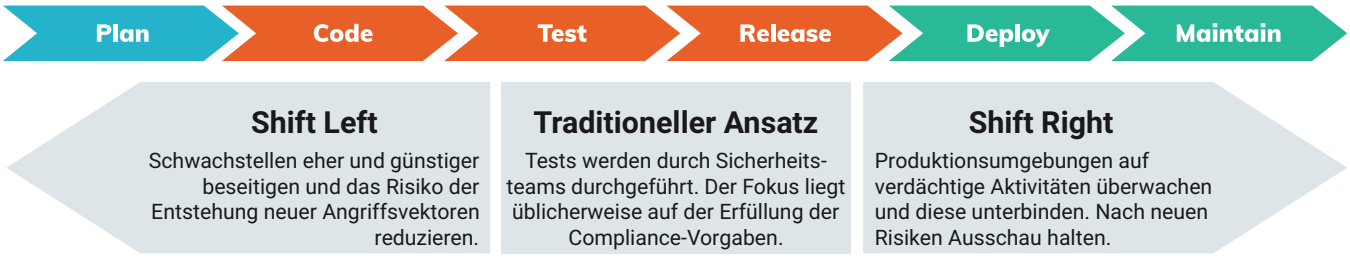


Figure 5: Shift Left vs Traditional vs Shift Right approach.

Aber wenn die Shift-Left-Mentalität schon seit einiger Zeit populär ist, warum sehen wir dann jetzt einen Trend zu Shift Right? Um das Entstehen einer "Shift Right"-Mentalität zu verstehen, muss man zunächst untersuchen, wie sich die Entwicklungsstile verändert haben. Anstelle des linearen Wasserfallmodells (populär in den 90er und frühen 2000er Jahren) ermöglicht DevOps jetzt die kontinuierliche Entwicklung und Bereitstellung von Software mit automatisierten Test- und Freigabeprozessen (im Gegensatz zu manuellen Prozessen).

Die Erwartung dabei ist, dass durch die Implementierung von DevOps alles reibungsloser abläuft, da die Software vor ihrer Freigabe automatisch auf Sicherheit getestet wird. Die Realität ist jedoch, dass automatisierte Test- und Freigabeprozesse die Sicherheit oft zugunsten von Geschwindigkeit und Effizienz vernachlässigen.

Daher erfordert die Sicherung von sich ständig ändernden Anwendungen (DevOps) eine Menge neuer Prozesse und Produktunterstützung, auf die die Dev-Teams weder vorbereitet sind noch die richtigen Tools haben, um die Sicherheit zu adressieren. Das bedeutet, dass die Sicherheit hinter das Entwicklungstempo zurückfällt. Wenn es nur eine Verschiebung nach links gibt, sind die Entwicklungsteams überlastet. Und die Statistiken lügen nicht; 47%[9] der Entwickler sagen, dass sie nicht genug Zeit für die Sicherheit haben.

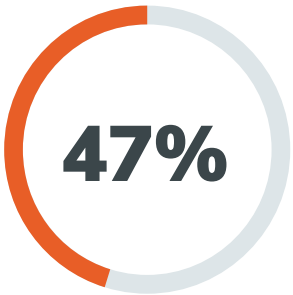


Figure 6: 47% of developers say they don't have time for security

Warum Shift Right wichtig ist

Während Shift Left die Qualität und die Erfüllung der Geschäftsanforderungen sicherstellt, werden das Funktionieren und die Performance in der realen Welt durch einen Shift Right-Ansatz gewährleistet. Shift Right verwendet einen kontrollierten experimentellen Ansatz, Tests in der produktiven Umgebung und konzentriert sich speziell auf Funktionalität, Leistung, Fehlertoleranz und Benutzererfahrung. Kurz gesagt, dadurch wird sichergestellt, dass die Testteams auf reale Benutzererfahrungen reagieren können, die in der Planungsphase des SDLC oft sehr schwer zu reproduzieren sind.

Shift Right testet eine gebaute und funktionierende Anwendung, die sich bereits im Einsatz und in der Postproduktionsphase befindet. Auf diese Weise können Organisationen Feedback unter realen Bedingungen sammeln, die viel stärker auf Leistung, Benutzerfreundlichkeit und Stabilität ausgerichtet sind. Auf diese Weise wird die Qualität der Anwendung auf der Grundlage der tatsächlichen Nutzung durch die Benutzer verbessert.

9 Securosis, Open Source Development and Application Security Survey Analysis (July 9, 2014)

Aber warum sollten Sie dies tun wollen?

Verbesserte Benutzererfahrung

Erfahrung ist im wahrsten Sinne des Wortes alles, ob Kunde oder Mitarbeiter; sie war in den letzten Jahren eine der größten Triebkräfte des Wandels. Bei der Anwendung eines Shift Right-Ansatzes werden Erfahrungen und Feedback gesammelt und dann sowohl aus geschäftlicher als auch aus technischer Sicht betrachtet. Auf diese Weise wird sichergestellt, dass alle Fragen individuell untersucht und auf dieser Grundlage verbessert werden können.

Umfang der Automatisierung

Wenn Zeit ein so kostbares Gut ist wie im Bereich der Sicherheit, ist die Automatisierung die Rettung. Die Automatisierung der Benutzerschnittstelle (UI) ist, sobald die Anwendung stark und stabil ist, entscheidend für ein schnelles Testen. Ein Shift Right-Ansatz bietet genau diese Plattform.

Breitere Abdeckung

Für eine bessere Qualität und Anwendungserfahrung müssen die Testteams mehr, öfter und so spät wie möglich testen. Ein Shift Right-Ansatz bietet eine viel breitere Testabdeckung mit Zugriff auf das komplette System, da dies in der Postproduktion geschieht. Vergleichen Sie dies mit dem Shift-Links-Ansatz, der in den Planungsphasen zum Tragen kommt, in denen es auf Zeit ankommt und Termine eingehalten werden müssen.

Welchen Weg soll ich gehen?

Im Zuge der Digitalisierung haben sich verschiedene Testansätze entwickelt. Daher gibt es einen Grund, an beiden Enden des SDLC-Spektrums aktiv zu werden. Mehr Tests, früheres Testen und breiteres Testen tragen alle dazu bei, ein brillantes Produkt zu entwickeln und damit den Aufstieg von SecDevOps als Praxis bei der Bereitstellung sicherer, stabiler und performanter Anwendungen zu unterstützen.

Auch in der digitalen Welt muss jedes Unternehmen, das diesen Namen verdient, sich um den Eindruck kümmern, den es bei seinen Kunden und Mitarbeitern hinterlässt. Und gerade jetzt, inmitten einer globalen Pandemie, könnte aus Sicht des Unternehmens nichts lebenswichtiger sein. Das Testen gleich zu Beginn des Anwendungs-Lebenszyklus und die anschließende Verfeinerung der Testfälle anhand des Benutzerfeedbacks in der Postproduktion sind für Unternehmen unerlässlich, um jede Form der digitalen Glaubwürdigkeit zu gewährleisten.

Wenn Zeit ein so kostbares Gut ist wie im Bereich der Sicherheit, ist die Automatisierung die Rettung.

https://www.rapid7.com/

TEIL 3

Best Practices für die Erkennung und Reaktion auf Bedrohungen

Die Erkennung von Bedrohungen und die Reaktion auf diese Bedrohungen haben für Sicherheitsteams seit jeher höchste Priorität. Sie müssen Risiken rechtzeitig erkennen und mit Hilfe umfangreicher Datenanalysen Bedrohungen aufspüren, damit sie wirksam auf Sicherheitsereignisse reagieren und Schäden eindämmen können. Und da in den letzten Monaten eine große Zahl von Menschen ins Home Office umgezogen ist, hat die Bedeutung von Threat Detection and Response noch zugenommen.

Als Folge der Verlagerung sind die üblichen Angriffsvektoren wie Phishing, Malware und Ransomware leider noch häufiger anzutreffen als zuvor. Um die Digitalisierung voranzutreiben, die Sicherheit der Menschen zu gewährleisten und den Geschäftsbetrieb aufrecht zu erhalten, ist Incident Detection und Abwehr eine noch kritischere Komponente der Business-Continuity-Planung.

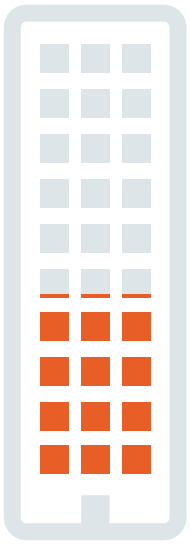
Herausforderungen in einer neuen Arbeitswelt

Diese seismische Verschiebung, die die Belegschaft mit mehr digitalen Fähigkeiten ausstattet, stellt Unternehmen vor wachsende Herausforderungen.

Heute plant über die Hälfte der Unternehmen, für den Fall künftiger Shutdowns mehr Anwendungen in die Cloud zu verlagern. Dies hat das Potenzial, die Angriffsfläche eines Unternehmens zu vergrößern und die Wahrscheinlichkeit von Fehlkonfigurationen zu erhöhen.

Die Implementierung eines dezentralen Arbeitsmodells erhöht auch die Zahl der Fehlalarme. Falschpositive weisen auf eine potenzielle Bedrohung hin, obwohl es eigentlich gar keine gibt. Sie haben zur Folge, dass ohnehin knappe Ressourcen für die Untersuchung von Vorfällen eingesetzt werden, die in Wirklichkeit nicht bedrohlich sind.

Die Ressourcen der Sicherheitsteams sind bereits begrenzt, und es wird geschätzt, dass es bis 2021 3.5 Millionen unbesetzte Stellen im Bereich der Cybersicherheit geben wird. Wenn Sicherheitsspezialisten beträchtliche Ressourcen investieren, um jede potenzielle Bedrohung zu untersuchen, sind sie nicht effizient oder produktiv, was möglicherweise zu Demotivation führt. Und obwohl die Notwendigkeit diktiert, wo Menschen gebraucht werden, sollten Organisationen bedenken, ob die iher Fähigkeiten optimal eingesetzt werden.



41%

OF COMPANIES USE BEST CYBERSECURITY PRACTICES

Figure 7: Only 41% of cyber security professionals said their companies are utilising best practices to ensure a secure remote workforce.

Die Verbesserung der digitalen Fähigkeiten bedeutet auch, sich mit einer Infrastruktur vertraut zu machen, die im Großen und Ganzen ungewohnt sein könnte. Obwohl ein beträchtlicher Teil der Unternehmen bereits in der Cloud operiert, erwägen viele von ihnen eine Beschleunigung ihrer Pläne zur Erweiterung dieser Infrastruktur. Und es kommt darauf an, dies richtig zu machen. Umfragen zufolge setzt weniger als die Hälfte der Unternehmen Best Practices ein, um Remote-Arbeitsplätze abzusichern. Dies kann zu schlecht konfigurierten Systemen führen oder riesige Löcher in Ihre Abwehrsysteme reißen.

Best Practices für Threat Detection and Response

Wenn Sie sich Fragen gestellt haben wie: “Müssen wir unsere Sicherheitsstrategie überdenken?”, “Was sind unsere größten Risiken?” und “Worauf sollte ich unsere Bemühungen konzentrieren?”, dann ist ein Cybersecurity Maturity Assessment (CSMA) ein guter Ausgangspunkt.

CSMA bietet Ihnen eine Lückenanalyse und Risikobewertung, wobei zur Beantwortung eben dieser Fragen bewährte Verfahren der Cybersicherheit und anerkannte Cyber-Frameworks verwendet werden. Es gibt Ihnen einen Überblick über Ihre aktuelle Sicherheitslage, eine objektive Überprüfung Ihrer bestehenden Pläne und einen Leitfaden für die strategische Sicherheitsplanung. Das Ergebnis hilft Ihrer Organisation bei der Entwicklung taktischer und strategischer Richtungen, um Ihre Bemühungen um Sicherheitsprogramme weiter auszureifen und zu stärken.

Aber wie lässt sich dies in die Praxis umsetzen? Welche Best Practices können Sie sich heute ansehen, um Ihrer Organisation bei der Anpassung zu helfen?

i.) Menschen: Geben Sie Ihren Teams Autonomie und stellen Sie die nötigen Werkzeuge und Ressourcen bereit

Geben Sie Ihren Teams die Autonomie, die sie brauchen, indem Sie sie mit leistungsstarker Technologie und Ressourcen ausstatten. So können sie ihre Arbeit rationalisieren und sich auf die wichtigen Dinge konzentrieren. Wenn Sie in die richtigen Lösungen investieren und bei der Auswertung von Warnmeldungen den richtigen Ansatz wählen, erhalten Ihre Teams die Fähigkeiten, die sie benötigen, um die Widerstandsfähigkeit Ihrer Organisation zu stärken.

Automatisierung kann zum Beispiel eine große Rolle spielen, wenn es darum geht, die alltäglichen Sicherheitsaufgaben zu erledigen und ihnen gleichzeitig mehr Freiraum für höherwertige Aufgaben zu verschaffen. Sie rationalisiert sich wiederholende, manuelle Aufgaben zu kohärenten und automatisierten Arbeitsabläufen. Durch die Einbindung einer Reihe von Aufgaben in ein automatisiertes System (z.B. bei Phishing-Untersuchungen) werden Sicherheitsprozesse effizienter und weniger anfällig für menschliche Fehler.

Durch die höhere Effizienz, die sich aus der Automatisierung ergibt, können bessere und schnellere Entscheidungen getroffen werden, was wiederum die gesamte Sicherheitslage Ihrer Organisation verbessert. Noch besser: Da sich wiederholende und manuelle Aufgaben durch die Automatisierung erledigt werden, können sich Sicherheitsspezialisten auf strategischere Arbeit konzentrieren und ihre Arbeitszufriedenheit steigern, was es wiederum Ihnen erleichtert, Top-Talente an sich zu binden.

Mehr Informationen zu Best Practices der Sicherheitsautomatisierung

ii.) Prozesse: Aufbau besserer Prozesse und Erfüllung von Compliance-Anforderungen

Effiziente Prozesse sind unerlässlich für eine starke Sicherheitsstrategie. Es ist von entscheidender Bedeutung, zu verstehen, was Sie tun müssen und was Sie tun sollten - und ob Sie alle Compliance-Anforderungen erfüllen.

Es gibt unterschiedliche Standards und Vorschriften, aber gehen diese weit genug, um Sie zu leiten und zu schützen? Für einige Unternehmen könnte die Frage lauten: “Verzichte ich auf stärkere Sicherheitsprozesse, um das Überleben meines Unternehmens zu sichern?

Beispielsweise haben Unternehmen in Branchen, die von der Pandemie besonders hart getroffen wurden, wahrscheinlich einen größeren Teil ihrer Tätigkeiten in eine digitale Umgebung verlagert. In dem Bestreben, das Überleben zu sichern und so viele Menschen wie möglich zu erreichen, werden dabei möglicherweise Technologien eingesetzt, von denen man nicht weiß, wie man sie richtig vor potenziellen Risiken schützt.

Die Top 20 Critical Security Controls (CIS) des Center for Internet Security sind eine hervorragende Möglichkeit, Ihre wichtigsten Sicherheitsfragen zu beantworten. Sie setzen reale Bedrohungsdaten in priorisierte und gangbare Wege um, auf denen Sie Ihr Unternehmen vor den häufigsten Angriffsmustern schützen können.

Mehr Informationen zu CIS Controls.

Das MITRE ATT@CK Framework wird weithin als Autorität für das Verständnis der Verhaltensweisen und Techniken anerkannt, die Hacker heute gegen Unternehmen einsetzen. Es beseitigt nicht nur Zweideutigkeiten und bietet ein gemeinsames Vokabular für Branchenexperten zur Diskussion und Zusammenarbeit bei der Bekämpfung gegnerischer Methoden, sondern bietet auch praktische Anwendungen für Ihre Sicherheitsteams.

Mehr Informationen zum MITRE ATT@CK Framework.

Technik: Einsatz von Partnern mit großem Technologieverständnis

Für viele Organisationen hat die Pandemie große Auswirkungen sowohl auf die Beschäftigten als auch auf die Budgets gehabt. Dennoch sind die Anforderungen an die Sicherheit und die Einhaltung von Vorschriften stark gestiegen. Managed Security Services sind eine großartige Möglichkeit, den Mangel an Zeit, Fachkräften und Technologie über einen Partner auszugleichen.

Managed Detection and Response zum Beispiel ermöglicht es Ihnen, das Fachwissen von Branchenexperten zu nutzen, um Ihr Sicherheitsprogramm reifen zu lassen und Ihre Position zu stärken. Entsprechende Dienstleister können Ihnen bei der Erkennung aktueller Bedrohungen durch mehrere fortschrittliche Erkennungsmethoden helfen, einschließlich Verhaltensanalyse und Analyse des Netzwerkverkehrs. Und sie können Risiken mit detaillierten, auf Ihr Unternehmen zugeschnittenen Berichten und Anleitungen sofort eindämmen, beheben und mindern.

Aber wie wählt man den richtigen Partner aus? Hier sind drei Dinge zu beachten:

Stellen Sie sicher, dass Ihre Auswahlliste Unternehmen enthält, die über außergewöhnliche Experten und die Technologie verfügen, um proaktiv auf die Jagd zu gehen. Sie brauchen erfahrene Experten, die schon alles gesehen haben, um in Ihrem Namen aktiv zu werden.

Stellen Sie sicher, dass der Partner eine kundenspezifische Lösung anbietet, die auf Ihre speziellen Risiken abgestimmt ist; keine Einheitslösung für alle.

Stellen Sie sicher, dass sie Anleitung und Unterstützung bieten, um zu reagieren und Abhilfe zu schaffen. Wenn Sie Angreifer in Ihrer Umgebung finden, ist es von entscheidender Bedeutung, dass Sie schnell von der Entdeckung zur Reaktion und Abhilfe übergehen. Eine umfassende Managed Detection and Response wird genau das tun.

Mehr Informationen zu Managed Services

Warum Sie Ihren D&R-Ansatz neu bewerten sollten

Zwar hat die Pandemie viele dazu veranlasst, ihre Sicherheitshaltung zu überdenken, doch Veränderungen finden ständig statt. Ihre Sicherheitsstrategie sollte immer als bewegliches Ziel betrachtet werden, da sich die Marktbedingungen ändern.

Gelegentlich werden Sie wahrscheinlich risikofreudiger sein, wenn sich Innovationen durchsetzen. Doch auf der anderen Seite hat Sicherheit Vorrang vor der Notwendigkeit von Skalierung und Innovation. Wo auch immer Sie sich auf Ihrer Sicherheitsreise befinden, es wird immer sinnvoll sein, Ihre Sicherheitshaltung im Lichte dieser einfachen Best Practices zu betrachten.

Ihre Sicherheitsstrategie sollte immer als bewegliches Ziel betrachtet werden, da sich die Marktbedingungen ändern.

https://www.rapid7.com/

RAPID7

www.rapid7.com