MATRIX42

Unbekannte Sicherheitslücken erkennen und schließen

Wie ein IT-Asset Management mit kontinuierlicher Überwachung und Erkennung Unternehmen gegen bisher unbekannte Sicherheitsrisiken schützt

Whitepaper

Cyber-Attacken auf dem Höchststand

Seit dem Beginn der COVID19-Pandemie und dem hektischen Umzug vieler Mitarbeiter ins Home-Office, haben Ransomware Angriffe um ca. 50% zugenommen.[1] Phishing-Attacken wie z. B. gefälschte Virenwarnungen von Microsoft gehen mit fast 193 Millionen durch die Decke.[2] Besonders alarmierend: die Zunahmen von sog. Insider Attacken. Laut Studien ist mehr als jedes zweite Unternehmen durch Daten-Diebstahl aus den eigenen Wänden betroffen.[3]

Alle Fälle haben eines gemeinsam: Trotz hoher Investitionen bleiben die meisten Cyber-Attacken lange unentdeckt. In vielen Fällen wurde ein immenser wirtschaftlicher Schaden verursacht. Allein 2019 summierte sich der Schaden nur für deutsche Unternehmen auf über 100 Milliarden Euro.[4]

IT-Organisatoren müssen heutzutage einen Spagat hinlegen. Sie sollen einerseits als digitaler Business Enabler agieren, neue Services in Rekordzeit bereitstellen und digitales Arbeiten auf Knopfdruck ermöglichen. Anderseits müssen sie eine steigende Vielfalt an Endgeräten, Applikationen und Zugängen gegen eine zunehmende Anzahl ausgeklügelter Cyberattacken schützen. Bei meist gleichbleibendem Personal und ohne das die Security Tools die Produktivität der Mitarbeiter stören. Nicht einmal das allerbeste IT-Team kann das zu 100% leisten.

Jedes Business ist mittelweile ein digitales Business, IT Security ist die Lebensversicherung der digitalen Welt. Potenzielle Sicherheitsrisiken für unternehmenskritische Systeme, Daten und Infrastrukturkomponenten frühzeitig zu erkennen, beurteilen und schnell beheben zu können, ist eine Daueraufgabe für jede IT-Führungskraft. Dieses Whitepaper zeigt, wie Unternehmen durch ein modernes IT-Asset Management (ITAM) mit kontinuierlicher Überwachung und Erkennung eine höhere Transparenz und Reaktionsfähigkeit erzielen, um ihre kritischen Unternehmensdienste auch vor bisher unbekannten Sicherheitsrisiken zu schützen.

Sie können nicht etwas bekämpfen, das Sie nicht sehen

Durch die COVID-19-Pandemie arbeiten zunehmend mehr Mitarbeiter von zu Hause aus. Dabei ist der Trend ist nicht neu: Bereits vor der Pandemie haben 50% aller Mitarbeiter weltweit an mehr als zwei Tagen von außerhalb des Büros gearbeitet. Experten gehen sogar davon aus, dass innerhalb der nächsten 10 Jahre die Hälfte des Personals als Freelancer arbeiten wird.[5]

Angesichts der wachsenden Bedeutung von Fernarbeit nutzen immer mehr Mitarbeiter eine Vielzahl von neuen Anwendungen und Endgeräten. Doch die eigene Umgebung birgt auch Risiken hinsichtlich der Netzwerksicherheit: unzureichend gesicherte WLAN-Netzwerke und Datenverbindungen, die Nutzung von ungesicherten (privaten) Geräten oder mangelhaft konfigurierte Firewalls bedeuten gravierende Sicherheitsrisiken sowohl für die Endpunkte als auch für zentrale Teile der IT-Infrastruktur.

- **Drei Viertel aller Unternehmen, in denen Mitarbeiter von zu Hause arbeiten, haben angegeben, dass es länger dauert potenzielle Datenschutzverletzungen zu identifizieren und einzudämmen.[6]**

- **Neun von zehn Datenlecks entstehen nicht durch Probleme beim Cloud-Dienstanbieter, sondern durch menschliche Fehler von Mitarbeitern.[7]**

[1] Checkpoint Blog: Global Surges in Ransomware Attacks
[2] Zscaler, 2020: The State of Encrypted Attacks
[3] 2020 Cost of Insider Threats: Global Report
[4] BITKOM-Studienbericht 2020 - Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt
[5] IWP Workplace Survey. March 2019.
[6] Cost of a Data Breach Report. IBM & Ponemon Institute. 2020.
[7] Kaspersky Lab Global Corporate IT Security Risks Survey. 2019.

Cloud-, Multi-Cloud- und Hybridumgebungen

Fernarbeit ist nicht die einzige Herausforderung, die Unternehmen dazu zwingt, ihre Sicherheitsstrategie neu auszurichten. Mit zunehmender Nutzung von Cloud-Diensten setzen sie sich zusätzlichen Risiken aus, die mit Multi-Cloud- und Hybridumgebungen verbunden sind. Dazu gehören die Speicherung sensibler Daten, Fehler von Mitarbeitern und Sicherheitslücken in der Cloud-Infrastruktur. IT-Teams müssen die Umsetzung digitaler Arbeitsplatz- und Geschäftsmodelle vorantreiben und gegen Sicherheits-Risken absichern, die sie nicht ohne Weiteres erkennen können. In den Bereichen IT-Asset Management und Netzwerksicherheit gibt es verschiedene Herausforderungen, welche die Erkennung und Abwehr von Bedrohungen erschweren. Zum Beispiel:

Unvollständiger IT-Asset-Bestand

Die meisten Erkennungs-Tools finden nicht alle Arbeitsplatzrechner, Sicherheitsgeräte, Drucker und andere IT-Assets, wenn diese nur temporär oder unregelmäßig mit dem Netzwerk verbunden sind. Im besten Fall nutzen die Erkennungs-Tools IP-Adressen im Subnetz oder anderen vordefinierten Orten und Entitäten. Andere IP-Adressen im Netzwerk, die sich außerhalb des definierten Bereiches oder Subnetzes befinden, werden bei Scans jedoch nicht erfasst und somit übersehen. Beispiel hierfür sind sogenannte Jump-Hosts außerhalb eines Subnetzes, die sich mit Servern im Subnetz verbinden.

Die rasante Zunahme von Multi-Cloud- und Hybridinfrastrukturen erhöht die potenzielle Angriffsoberfläche, da noch mehr Endpunkte verwaltet und überwacht werden müssen. In diesen Szenarien benötigen IT-Teams einen lückenlosen Überblick über alle IT-Assets des Unternehmens, auch um jederzeit einen vollständigen und aktuellen Inventar-Bestand sicherstellen zu können.

Eingeschränkte Netflow- und IP-Datenstrom-Transparenz

IT-Teams können oft nicht genau erkennen, welche Anwendungen und Geräte im Netzwerk kommunizieren, da ihre Erkennungs-Tools nicht wissen, wo sie suchen müssen. Viele Anwendungen und Geräte wurden entweder noch nie identifiziert oder können mit herkömmlichen Erkennungs- und Überwachungstools nicht erfasst werden. Eine mangelhafte Transparenz über die IP-Datenströme führt dazu, dass IT-Teams nicht genau wissen, welche Dienste an welchen Standorten ausgeführt werden und potenziell sensible Daten übertragen. Daher können sie die Integrität verschiedener Dienste nicht ausreichend nachverfolgen.

Nur intervallweise Scans statt Echtzeit-Überwachung

Herkömmliche Erkennungs-Tools scannen nur wenige Male pro Woche, Monat oder Quartal nach IT-Assets in den Netzwerk-Umgebungen. Unabhängig vom veranschlagten Intervall sind diese Scans nie ausreichend, um auch alle temporären IT-Assets zu erkennen, die sich mit dem Netzwerk verbinden. Dazu gehören BYOD-Laptops und Smartphones, Netzwerkdrucker, Kameras, virtuelle Computer, temporäre Server und Switches sowie viele weitere Geräte.

- 43% aller Sicherheitsverletzungen entstehen durch Angriffe auf Webanwendungen[8]
- ca. 30 % aller Mittelstands- und 20 % aller Großunternehmen haben keine oder nur unzureichende Absicherung zum Schutz Ihrer gespeicherten Daten in der Cloud[9]

Da herkömmliche Lösungen nicht jede Anmeldung am VPN tracken, können diese Tools auch nicht erkennen, ob es sich bei einer VPN-Anmeldung um einen Hack eines potenziellen Angreifers oder eines nicht zugangsberechtigten Mitarbeiters handelt, der Zugangsdaten klont oder Daten stiehlt. Cloud-Migrationen sind eine weitere Herausforderung für IT-Teams, da in den Migrationsplänen möglicherweise Abhängigkeiten auf VPN-Verbindungen fehlen, die bei regelmäßigen Scans ebenfalls nicht erkannt werden.

Nachlässige Sicherheitspraktiken

Wenn die IT-Assets eines Unternehmens nur manuell verwaltet, ihr Bestand nur unregelmäßig aktualisiert oder keine Abhängigkeiten der IT-Assets untereinander erfasst werden, erschwert dies die Einsicht in die Angriffsoberfläche und verzögert die Reaktion auf Bedrohungen. Möglicherweise werden IT- Assets nur unregelmäßig oder im Rahmen von Compliance-Anforderungen oder Audits aktualisiert. In der Zeit, wo ein IT-Asset entweder manuell hinzugefügt oder aktualisiert wird, herrscht im Netzwerk ein lebhaftes Kommen und Gehen von neuen IT-Assets, etwa aufgrund von Rechenzentrumskonsolidierungen oder Außerbetriebnahmen.

Parallel dazu decken Lösungen für Application Performance Management (APM), Security Information and Event Management (SIEM) und Netzwerkerkennung nur die wichtigsten Infrastrukturkomponenten ab. Sie sind oft nicht mit der IT-Asset Management-Lösung für die Verwaltung und Erkennung von IT-Assets integriert. Daher existiert keine umfassende Echtzeit-Ansicht auf die gesamte Umgebung der IT-Infrastruktur. Das verzögert die Erkennung und Identifizierung möglicher Sicherheitsvorfälle, da IT-Teams Berichte und Benachrichtigungen aus verschiedenen Systemen nur mit beträchtlichem Zeit- und Arbeitsaufwand miteinander kombinieren und auswerten können.

[8] Data Breach Investigations Report. Verizon. 2020.
[9] Kaspersky Lab Global Corporate IT Security Risks Survey. 2019.

Unvollständiges und inakkurates IT-Asset Management kann richtig teuer werden

Wenn IT-Teams IT-Assets nicht ordnungsgemäß und korrekt verwalten können, ist das gesamte Unternehmen wesentlich anfälliger für Cyberattacken. Hier sind exemplarisch einige Risiken genannt, die aufgrund eines auf mangelhaften Sicherheitspraktiken basierenden IT-Asset-Managements entstehen können.

Datenschutzverletzungen und Datenverluste

Angreifer können mühelos wertvolle IT-Assets ins Visier nehmen, mit denen kritische Unternehmensdienste und Anwendungen bereitgestellt werden. Beispiele hierfür sind Online-Bestellsysteme, in denen Einkäufe und finanzielle Daten von Kunden gespeichert werden, Patientendatensätze oder andere personenbezogene oder private Daten. Ebenso besorgniserregend sind mangelhaft konfigurierte Firewall-Richtlinien, die keinen Alarm schlagen, wenn sich Eindringlinge im Netzwerk befinden oder ein Angreifer Daten aus dem Netzwerk herausleitet. Datenschutzverletzungen können verheerende finanzielle Folgen haben. Eine einzige Datenschutzverletzungen kostet US-Unternehmen heutzutage durchschnittlich 8 Millionen US-Dollar, das sind 5,3% mehr als vor einem Jahr.[10]

Ungeplante Ausfälle

Schadsoftware, DDoS und andere Angriffe können Unternehmensdienste je nach Größe und Umfang des Angriffs komplett vom Netz nehmen. Ungeplante Ausfälle können ein Unternehmen auch schnell ins finanzielle Chaos stürzen. Laut aktueller Forschungsergebnisse belaufen sich die Kosten für Ausfälle auf beinahe 9.000 US-Dollar pro Minute.[11] Dieser Betrag kann je nach Branche, Unternehmensgröße und Geschäftsmodell noch deutlich höher ausfallen.[12] Ausfälle können außerdem das Ansehen der Marke beschädigen, wodurch ebenfalls starke Umsatzverluste entstehen können. Beinahe 40 % der Gesamtkosten bei Datenschutzverletzungen und Datenverlusten sind die Folge von entgangenen Umsätzen.[13]

„Durch Social Media werden Service-Ausfälle heutzutage weltweit innerhalb von Minuten bekannt, nicht erst nach Stunden oder Tagen."

David DiCristofaro, KPMG

Compliance-Verletzungen

Zum Schutz von Daten und der Privatsphäre sowie damit verbundener Sicherheitsmaßnahmen müssen Unternehmen zahlreiche gesetzliche Vorgaben erfüllen, wie etwa:

- PCI
- HIPAA
- SOC
- DSGVO
- ISO
- FISMA

Lückenhaftes IT- Asset Management kann dazu führen, dass Unternehmen anfälliger für Netzwerkangriffe sind und dadurch Compliance-Vorgaben verletzen sowie empfindliche Strafzahlungen riskieren.

- Die durchschnittlichen Kosten für Compliance-Verletzungen in internationalen Unternehmen belaufen sich auf 14,82 Millionen US-Dollar.[14]

Top-Anwendungsfälle für moderne und umfassende IT-Asset Management-Lösungen

- IT-Service Management (ITSM)
- Cloud-Migration
- Rechenzentrums- und Cloud-Optimierung
- IT-Governance
- Einhaltung gesetzlicher Vorgaben
- Kostenoptimierung
- Verwaltung der Sicherheitskonfiguration
- Zusammenschlüsse und Übernahmen

[10] Cost of a Data Breach Report. IBM & Ponemon Institute. 2020.
[11] Cost of Data Center Outages. Vertiv & Ponemon Institute. January 2016.
[12] Calculating the cost of downtime. Atlassian.
[13] Cost of a Data Breach Report. IBM & Ponemon Institute. 2020.
[14] The True Cost of Compliance with Data Protection Regulations. Globalscape & Ponemon. December 2017.

Modernes IT-Asset Management und Netzwerksicherheit für neuartige Bedrohungen

Durch die Weiterentwicklung herkömmlicher Tools für das IT-Asset Management (ITAM) zu einer modernen und umfassenden Lösung sind IT-Teams in der Lage, den vielfältigen Sicherheitsanforderungen in einer zunehmend gefährlicheren Cyberlandschaft zu begegnen und vor Sicherheitsrisiken schützen, die bisher unbemerkt geblieben sind.

- Die passive und aktive IT-Asset-Erkennung bietet eine 360 Grad Ansicht der kompletten IT-Landschaft in Echtzeit und verbessert die Transparenz sowie schnellere Erkennung potenzieller Risiken.
- Dank der Transparenz auf Paketebene können IT-Teams jederzeit erkennen, wann Server, Switches oder andere vernetzte Geräte das Netzwerk betreten oder verlassen oder mit anderen IT-Assets kommunizieren, um bisher verborgene IT-Assets zu finden, die ein potenzielles Sicherheits-Risiko darstellen können.
- Durch eine zentrale Informationsquelle wird der Upload-Prozess zu den CMDBs automatisiert und vereinfacht.
- Die erweiterte virtuelle Perimeter-Sicherheit erkennt autorisierte und unbefugte Änderungen an der IT-Infrastruktur in Echtzeit, womit IT-Teams schneller auf Bedrohungen reagieren können.
- Die Integration mit SIEM-Tools erkennt neue Formen der Netzwerkkommunikation mit unternehmenskritischen Systemen und Diensten, auf denen sich sensible Daten befinden, um Auswüchse von Schatten-IT zu unterbinden.
- Die verbesserte Transparenz unterstützt IT-Teams bei der Konsolidierung von IT-Assets und erlaubt die bessere Planung bei der Anschaffung von Softwarelizenzen.
- Branchenweite bewährte Methoden wie etwa die Vorgaben des Center for Internet Security (CIS) verbessern die Bestandskontrolle für Hardware und Software.

In 4 Schritten zu einer effektiven IT-Asset Management-Lösung

Je nach aktueller Sicherheitsstrategie und verfügbaren Ressourcen müssen neue IT-Asset Management-Initiativen in vielen Unternehmen phasenweise eingeführt werden. Durch einen methodischen und schrittweisen Ansatz können die Unternehmen die Kontrolle über ihr IT-Asset Management erlangen und fortlaufend verbessern, und gleichzeitig Alt-Systeme und -methoden ablösen. Mit den folgenden Schritten können Unternehmen die Effektivität ihres IT-Asset Managements verbessern:

1. IT-Assets erkennen und CMDBs und ITSM integrieren

Für eine unternehmenskritische Sicherheitsstrategie ist es entscheidend, dass alle IT-Assets im Netzwerk jederzeit exakt erfasst und identifiziert werden. Mit einer Kombination aus passiven und aktiven Erkennungsmethoden können Sie Geräte in Echtzeit erkennen, identifizieren und mit Konfigurationsverwaltungsdatenbanken (CMDBs) und ITSM-Lösungen synchronisieren, um Incidents schneller zu beheben und Verfügbarkeit und Kundenzufriedenheit zu verbessern.

2. Abbildung von Geräten und Abhängigkeiten, die Business-Dienste bereitstellen

Ein Mapping-Tool scannt den Datenverkehrsfluss im Netzwerk passiv und ermittelt so alle Server und Geräte, die innerhalb einer Anwendung oder eines Dienstes miteinander kommunizieren, um anschließend automatisch Service-Anordnungen zu erkennen und zu empfehlen, ohne Vorkenntnisse oder Eingaben eines Anwenders. Durch eine Basiserhebung (Baseline) aller IT-Assets können im Anschluss Änderungen und Bedrohungen an der IT-Landschaft in Echtzeit sofort erkannt werden.

3. Leistungsüberwachung, um Serviceausfälle zu vermeiden

Unternehmen sollten die Integrität und Verfügbarkeit ihrer Server, Anwendungen, Speichermedien und Netzwerkgeräte sowie der restlichen Infrastruktur kontinuierlich überwachen, um Service-Unterbrechungen durch verdächtige Aktivitäten, defekte Geräte sowie autorisierte und/oder unbefugte Änderungen proaktiv zu vermeiden. Wenn eine Anwendung oder ein IT-Asset von den in der Basiserhebung (Baseline) ermittelten Datenbestandes abweicht, wird automatisch eine Benachrichtigung generiert und an ein Tool oder einen Workflow gesendet.

4. IT an Unternehmenszielen ausrichten

Für die Zukunft ist es wichtig, dass sich Integrität und Leistung von unternehmenskritischen Diensten an den Unternehmenszielen ausgerichtet werden, um Risiken zu senken und Dienste zu schützen, erfolgreiche Cloud-Migrationen zu planen und kostspielige Serviceausfälle zu vermeiden.

Secure Discovery and Dependency Mapping: Eine sicherheitsorientierte IT-Asset Management-Lösung für Unternehmen

Secure Discovery and Dependency Mapping ist die erste Sicherheitslösung für Unternehmen, die Echtzeit-Informationen zu Anwendungen, IT-Assets und deren Abhängigkeiten auf Business Services aus einer Plattform bereitstellt, um Netzwerke zu schützen und die Service-Bereitstellung zu verbessern. Die integrierte Plattform verbessert die Transparenz und die Sicherheit für IT-Asset Management, Konfigurationsverwaltung, Cloud-Migrationen und IT-Service-Management-Migrationen.

- Umfang und Details von aktuellen und vergangenen Änderungen an Unternehmensdiensten.
- Welche Unternehmensdienste sind von einer geplanten Änderung betroffen und auf welche Art?
- Übertragungsdaten auf Paketebene mit Einblicken in Paketkopfzeilen für mehr Transparenz im Netzwerkdatenfluss.
- Zusammenhänge zwischen Störungen und Anfragen für die ITSM-Lösung und Unternehmensdienste.
- Erkennen von Veränderungen an Unternehmensdiensten in Echtzeit, damit Supportteams insbesondere in dynamischen Infrastrukturen jederzeit aktuell informiert sind.
- Nutzen Sie die agentenlose IT-Asset-Erkennung für mühelose und schnelle Bereitstellungen und eine nahtlose Einführung.
- Erstellen Sie eine Basis-Übersicht der Business Services inklusive ihrer zugeordneten und vernetzten IT-Assets und überwachen Sie Zu- und Abgänge von Komponenten, um jederzeit eine vollständige Abbildung Ihrer IT-Assets und Abhängigkeiten erstellen zu können.
- Erkennen, identifizieren und bilden Sie die Beziehungen zwischen vernetzten IT-Assets, die an der Bereitstellung eines Unternehmensdienstes beteiligt sind.
- Beobachten Sie die Verhaltensweisen von Entitäten und Abhängigkeiten, und erstellen Sie Benachrichtigungen bei Änderungen an der Baseline-Karte, um Hinweise auf Angriffe und kompromittierte Elemente zu identifizieren und die Netzwerkaktivität bei autorisierten und unbefugten Änderungen jederzeit zu überblicken.
- Überwachen Sie den Datenfluss im Netzwerk fortlaufend, um Bedrohungen für wertvolle Assets durch Lateral Movement, Insider und unerwünschte Geräte zu erkennen.

IT-Sicherheit für Unternehmen war noch nie so anspruchsvoll, komplex und überlebenswichtig wie heute. IT-Teams müssen nicht nur Änderungen am Arbeitsplatz und ständig wechselnde Geschäftsanforderungen unterstützen, sondern auch immer mehr Endpunkte und IT-Assets erkennen und Bedrohungen abwehren, oft mit derselben Anzahl an Mitarbeitern und denselben Tools.

Homeoffice-Richtlinien und Multi-Cloud-Umgebungen führen zu mehr Komplexität und Security Schwachstellen. Altsysteme und bisherige IT-Prozesse reichen nicht mehr aus, um potenzielle Sicherheitsrisiken und -vorfälle zu vermeiden.

Daher sollten sich IT-Verantwortliche nach IT-Asset Management-Lösungen umsehen, um ihre vorhandenen Sicherheitskontrollen zu erweitern. Ein IT-Asset Management mit kontinuierlicher IT-Asset-Erkennung verbessert die Transparenz für die gesamte IT-Landschaft und sorgt dafür, dass IT-Teams proaktiv auf potenzielle Bedrohungen reagieren können, bevor ernsthafte Probleme auftreten.

Standorte

Hauptsitz Deutschland
Matrix42 AG
Elbinger Straße 7
60487 Frankfurt am Main
Deutschland
Telefon: +49 69 66773-8220
Fax: +49 69 66778-8657
info@matrix42.com

Niederlassung USA
FireScope, Inc.
412 Olive Ave, Suite 603 Huntington Beach, CA 92648
USA
Telefon: +1 657-204-0993
sales@firescope.com

Weitere Niederlassungen im Ausland finden Sie auf unserer Website: www.matrix42.com

Über Matrix42

Matrix42 unterstützt Organisationen dabei, die Arbeitsumgebung ihrer Mitarbeiter zu digitalisieren. Die Software für Digital Workspace Experience verwaltet Geräte, Anwendungen, Prozesse und Services einfach, sicher und konform. Die innovative Software integriert physische, virtuelle, mobile und cloudbasierte Arbeitsumgebungen nahtlos in vorhandene Infrastrukturen.

Die Matrix42 AG hat den Hauptsitz in Frankfurt am Main, Deutschland, und vertreibt und implementiert Softwarelösungen weltweit mit lokalen und globalen Partnern.

Webversion-Whitepaper-Unbekannte Sicherheitslücken erkennen und schließen-DE-202102