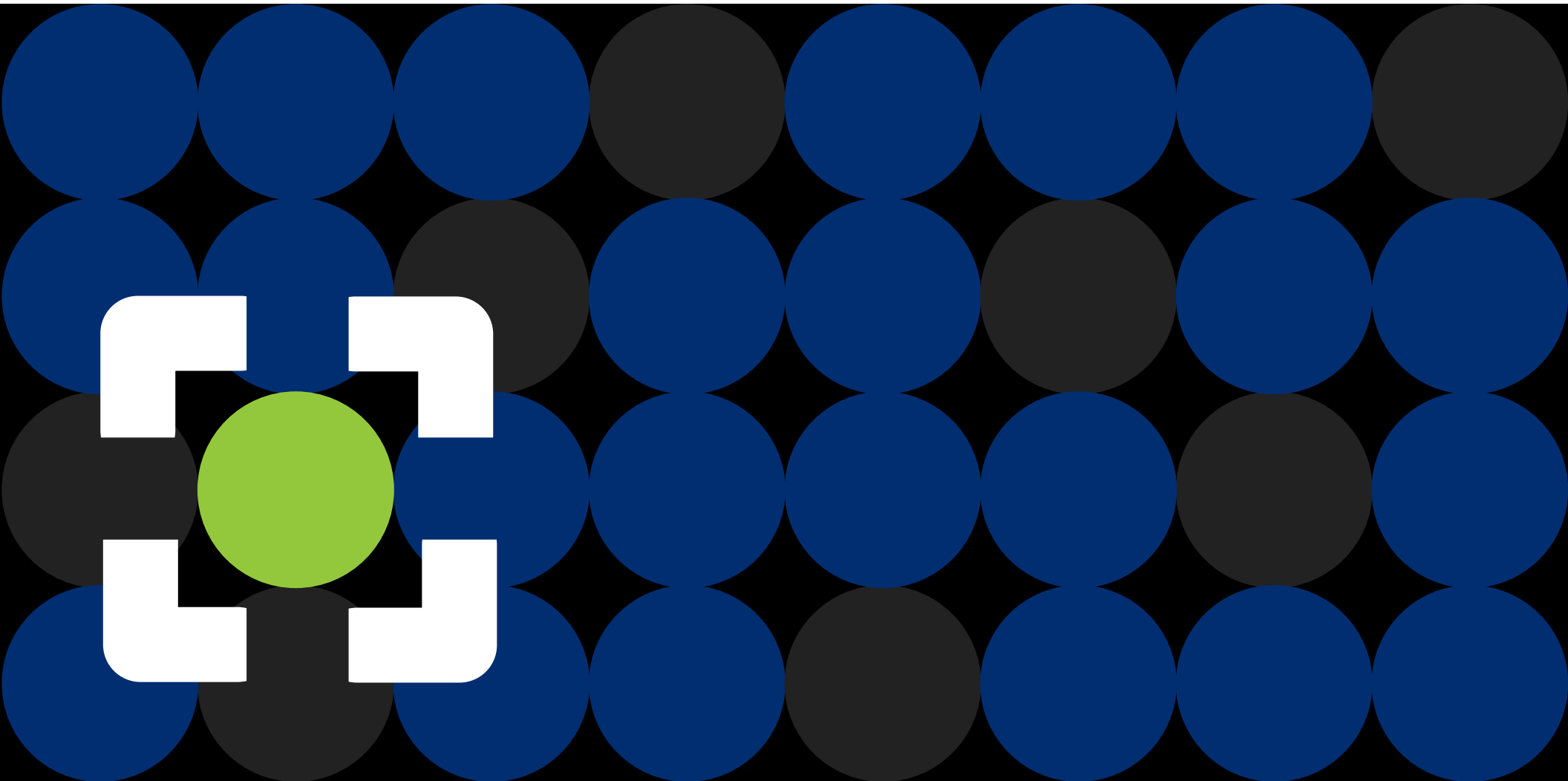
FORESCOUT
Active Defense for the Enterprise of Things™

Schutz für das Enterprise of Things
Fünf Herausforderungen bei der Absicherung des Netzwerks



INHALT

3 Einleitung

4 Herausforderung 1: Wie können Sie die enorme Menge an unverwalteten Geräten inventarisieren und verwalten?

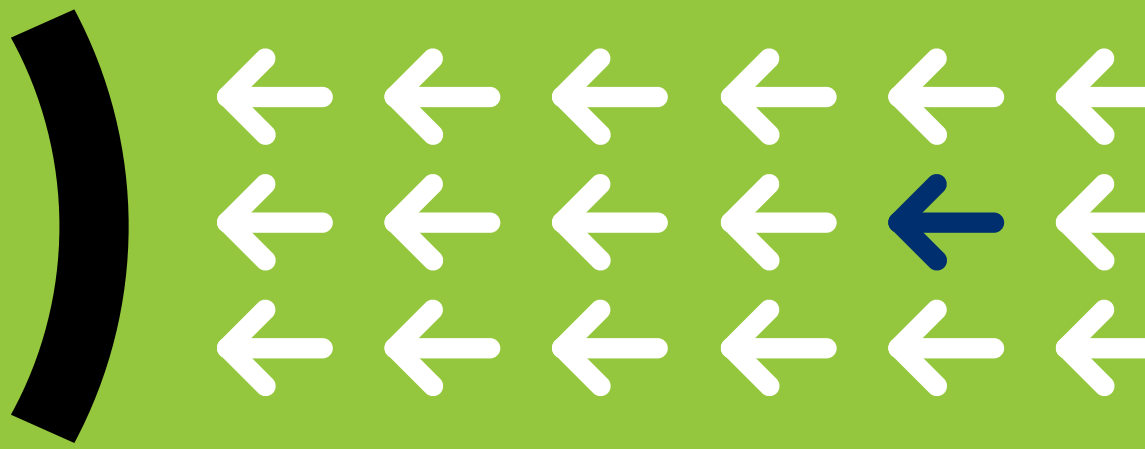
5 Herausforderung 2: Wo verbergen sich die Risiken in heutigen Unternehmensumgebungen?

6 Herausforderung 3: Der Netzwerkperimeter ist Geschichte – was nun?

7 Herausforderung 4: Segmentierung ist unabdingbar, doch wie wird sie richtig umgesetzt, ohne die Geschäftsabläufe zu unterbrechen?

8 Herausforderung 5: Wie kann das Paradox „mehr mit weniger erreichen“ adressiert werden?

9 Fazit



EINLEITUNG

In heutigen Unternehmensnetzwerken sind die Geräte kaum noch kontrollierbar: Sowohl ihre Anzahl (Milliarden!) als auch die verschiedenen Typen (IT, OT, IoT, BYOD) nehmen rasant zu. Einige sind verwaltet und bekannt, während andere nicht identifiziert werden und unerkannt aus dem Raster fallen. Die eigentlichen Gerätenutzer sind hingegen querbeet verteilt: Mitarbeiter, Auftragnehmer, Partner und Kunden verbinden sich von jedem Ort mit dem Rechenzentrum oder der Cloud – und nicht alle nutzen sichere Verbindungen.

All das macht jede Netzwerkumgebung kompliziert: Ein echtes **Enterprise of Things** (Unternehmen der Dinge, EoT) benötigt wohl überlegte Planung und gut definierte Maßnahmen für die Absicherung der Geräte sowie des Unternehmens selbst.

Daraus folgen die fünf wichtigsten EoT-Herausforderungen, die heutige CISOs und andere Sicherheitsverantwortliche berücksichtigen müssen, sowie pragmatische Empfehlungen zur Bewältigung dieser Herausforderungen.

HERAUSFORDERUNG 1

Wie können Sie die enorme Menge an unverwalteten Geräten inventarisieren und verwalten?

> **Experten gehen davon aus, dass allein im Verlauf des Jahres 2020 weltweit 31 Milliarden IoT-Geräte installiert werden.**
>
> ***SECURITY TODAY*, 13. JANUAR 2020[1]**

> **„Laut 62 % der Umfrageteilnehmer werden Verbesserungen bei der Sicherheitslage des eigenen Unternehmens zunehmend von der Konver genz der IT- und OT-Kontrollsysteme abhängen."**
>
> **PONEMON INSTITUTE, FEBRUAR 2019[2]**

Verwaltete Geräte mit integrierten Sicherheitsagenten (z. B. unternehmenseigene PCs, Laptops und Smartphones) machen einen immer geringeren Anteil gegenüber den Milliarden von agentenlosen IoT- und OT-Geräten (operative Technologie) aus, die in die Netzwerke strömen. Gleichzeitig findet eine IT/OT-Netzwerkkonvergenz statt, die einerseits die Produktivität steigert und die Netzwerkverwaltung erleichtert, dabei jedoch auch zu neuen Risiken führt. Es ist schwerer als je zuvor, die Angriffsflächen heutiger heterogener Netzwerke zu schließen.

Empfehlungen:

- Stellen Sie fest, welche Tools 100 % Gerätetransparenz ohne blinde Flecken bieten.
- Schränken Sie Ihre Auswahl auf Lösungen ein, die agentenlose Prüfungen des Gerätezustands in Echtzeit erlauben.
- Unterstützen Sie Ihre Sicherheits- und IT-Mitarbeiter durch ein Echtzeit-Geräteinventar.

HERAUSFORDERUNG 2

Wo verbergen sich die Risiken in heutigen Unternehmensumgebungen?

> **„Intelligente Gebäude, medizinische Geräte, Netzwerktechnik und VoIP-Telefone sind die IoT-Geräte mit dem größten Risiko.“**
>
> **FORESCOUT RESEARCH, MAI 2020[3]**

> **„IoT- und netzwerkfähige Geräte haben zu neuen Kompromittierungsmöglichkeiten für Netzwerke und Unternehmen geführt. [...] Sicherheitsteams müssen jedes Gerät im Netzwerk permanent isolieren, absichern und kontrollieren.“**
>
> **FORRESTER RESEARCH, JUNI 2020[4]**

Das Konzept der Risikoanalyse verändert sich und passt sich an Ihre Angriffsflächen an. Eine aktuelle Forescout-Analyse zum Enterprise of Things zeigte, dass IoT-Geräte Ihr größtes Risiko darstellen. „Diese Geräte lassen sich nicht nur schwer überwachen und kontrollieren, sondern führen auch zu Schwachstellen an Punkten, wo sie die physische und digitale Welt verbinden. IoT-Geräte können als versteckte Hintertüren in Netzwerke missbraucht werden oder zu Hauptangriffspunkten von gezielter Malware werden.“[3]

Empfehlungen:

- Nutzen Sie Risikoanalysen, die mehrere Faktoren berücksichtigen, um Ihre Angriffsflächen zu identifizieren.
- Implementieren Sie eine aktive Sicherheitsstrategie, die auf Zero Trust basiert.
- Beschleunigen Sie die Reaktion auf Bedrohungen, indem Sie Warnungmeldungen je nach Risikoeinstufung priorisieren.
- Auch hier gilt: Vollständige Gerätetransparenz ist unverzichtbar.

HERAUSFORDERUNG 3

Der Netzwerkperimeter ist Geschichte – was nun?

> **„Zur Absicherung des Netzwerkperimeters in Unternehmen müssen neue Empfehlungen umgesetzt werden.“**
>
> **GARTNER, MAI 2020[5]**

Offen und trotzdem sicher? Wie soll das bei Netzwerken, welche nicht nur Campus, sondern auch Rechenzentren sowie Cloud- und OT-Umgebungen umfassen, überhaupt möglich sein? Seitdem Unternehmensnetzwerke sich bis an jeden Ort der Welt erstrecken, an dem sich Workloads und Mitarbeiter befinden, existiert kein absicherbarer Perimeter mehr. Wir sind heute an einem Punkt, an dem der Perimeter jedes verbundene Gerät und jeden Workload umgeben muss. Sicherheit beginnt am Edge der Ressource.

Empfehlungen:

- Schränken Sie mithilfe eines Least-Privilege-Modells wie Zero Trust die Zugriffe auf Unternehmensressourcen ein.
- Führen Sie für alle Geräte, die sich mit dem Netzwerk verbinden, unabhängig von deren Standort permanent Erkennungsmaßnahmen und Sicherheitsanalysen durch.
- Setzen Sie strenge richtlinienbasierte Konformitätsvorschriften für alle lokalen, BYOD- und Remote-Geräte durch.

HERAUSFORDERUNG 4

Segmentierung ist unabdingbar, doch wie wird sie richtig umgesetzt, ohne die Geschäftsabläufe zu unterbrechen?

> **„Wir gehen davon aus, dass 90 % der befragten Unternehmen in diesem Jahr Segmentierungsprojekte in Planung haben. Dieses Konzept stößt auf großes Interesse, doch nicht immer ist klar, wo begonnen werden soll, welche Risiken bestehen und ob das Ergebnis den finanziellen und zeitlichen Aufwand wert ist.“**
>
> **FORESCOUT RESEARCH, JANUAR 2019[6]**

Netzwerksegmentierung hatte jahrelang einen schlechten Ruf. Bis vor Kurzem ließen sich die verfügbaren Segmentierungstools nur mit großem Aufwand bereitstellen und konnten nicht domänenübergreifend agieren, sodass Geschäftsabläufe unterbrochen und Umgebungen fragmentiert wurden. Neue Geräte und die Ausdehnung der Netzwerke verschärften die Probleme zusätzlich. Mittlerweile gibt es jedoch zuverlässige Segmentierungslösungen, sodass ein Festhalten an anfälligen flachen Netzwerken nicht mehr notwendig ist.

Empfehlungen:

- Visualisieren Sie die Segmentierung und simulieren Sie Richtlinien vor deren Einsatz, um unnötige Unterbrechungen zu vermeiden.
- Gewährleisten Sie, dass Ihre Sicherheitslösung die Zero-Trust-Segmentierung jedes Geräts (einschließlich IT-, IoT- und OT-Geräte) an jedem Ort vereinfachen kann.
- Beschleunigen Sie die Implementierung von Zero Trust im gesamten Unternehmen.
- Wählen Sie eine moderne NAC-Plattform, die Netzwerksegmentierung ermöglicht.

HERAUSFORDERUNG 5

Wie kann das Paradox „mehr mit weniger erreichen“ adressiert werden?

> **„Unternehmen machen Fortschritte dabei, ihren Bestand an voneinander isolierten Sicherheitsprodukten zur Netzwerkverwaltung zu erringern. 64 % der Unternehmen nutzen jedoch noch im mer 4–10 Tools für Netzwerk-Monitoring und Problembehebung.“**
>
> **NETWORK MANAGEMENT MEGATRENDS 2020, APRIL 2020[7]**

> **„Bei den Unternehmensführungen ist das Interesse an Sicherheit und Risikomanagement so groß wie noch nie.“**
>
> **GARTNER RESEARCH, JULI 2019[8]**

Wenn das Sicherheits- und Netzwerkmanagement Ihres Unternehmens ein Sammelsurium isolierter und aufgabenspezifischer Legacy-Tools nutzt, ist es schwierig, Ihre SecOps-Abteilung als effizientes Bollwerk und Beitrag zur Kostensenkung zu präsentieren. Gleichzeitig können selbst sorgfältig ausgearbeitete Transformationspläne zu Problemen führen, seien es zähe Implementierung, geringe Rendite, steile Lernkurve und Unzufriedenheit mit den ausgewählten Lösungen. Zum Glück können Sie durch die Wahl der richtigen Plattform alle beteiligten Parteien – einschließlich des CFO – zufriedenstellen.

Empfehlungen:

Wählen Sie eine Plattform, die vorhandene Tools koordinieren kann und folgende Kriterien erfüllt:

- Schnelle, flexible Implementierung, die keine Störungen verursacht
- Schnelle Rendite
- Anbieterunabhängig – nutzen Sie Ihre vorhandene Infrastruktur
- Keine erzwungenen Software- oder Hardware-Upgrades
- Bietet Integrationen mit führenden IT- und Sicherheitsprodukten
- Agentenlose Erkennung von Geräten sowie Bewertung von Gerätesicherheit und Risiken
- Vermeidung von 802.1X-Komplexität und Verzögerungen bei der Bereitstellung sowie Senkung der Kosten
- Mit Wachstum des Unternehmens skalierbar
- Steigerung der Produktivität von Sicherheitsabläufen
- Agentenlose Transparenz, Kontrolle, Segmentierung und Zero Trust

Die größere Herausforderung hinter diesen 5 Herausforderungen

Jede der hier vorgestellten fünf Herausforderungen ist schwierig genug zu meistern. Ungelöst kann jede zur ultimativen Herausforderung führen – ein Cyberangriff, der operative Probleme, Datendiebstahl, Reputationsschaden, enorme Strafzahlungen, Bedrohungen der öffentlichen Sicherheit und viele weitere Probleme verursachen kann.

Das Zauberwort heißt Prävention, also eine effektive Lösung, die hundertprozentig agentenlose Gerätetransparenz, permanentes Monitoring und automatisierte Behebungsmaßnahmen bietet.

*Hinweise

1. *„The IoT Rundown for 2020: Stats, Risks, and Solutions"* (IoT-Zusammenfassung für 2020: Statistiken, Risiken und Lösungen), Security Today, 13. Januar 2020
2. *„Safety, Security & Privacy in the Interconnected World of IT, OT & IIoT"* (Sicherheit, Security und Datenschutz in der vernetzten Welt von IT, OT und IIoT), Forschungsbericht von Ponemon Institute, Februar 2019.
3. *„The Enterprise of Things Security Report, The State of IoT Security in 2020"* (Sicherheitsbericht für das Enterprise of Things, der Stand der IoT-Sicherheit für 2020), Forescout Research Labs, Mai 2020
4. *„Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles And Techniques"* (Abwehr von Ransomware mit Zero Trust: Stärkung des Schutzes mit Zero-Trust-Prinzipien und -Techniken), Forrester Research, 8. Juni 2020
5. *„Securing the Enterprise's New Perimeters"* (Absicherung des neuen Unternehmensperimeters), Gartner, 27. März 2020
6. *„Network Segmentation"* (Netzwerksegmentierung), Forescout-Blog, Januar 2019
7. *„Network Management Megatrends 2020"* (Die großen Trends beim Netzwerkmanagement 2020), Forschungsbericht von Enterprise Management Associates, April 2020
8. *„Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer"* (Fünf Fragen des Vorstands, die Sicherheits- und Risikoverantwortliche beantworten müssen), Gartner Research, Juli 2019

Nicht nur alles sehen, sondern alles schützen.

Kontaktieren Sie uns noch heute, damit Sie Ihr Enterprise of Things aktiv verteidigen können.

INFORMATIONEN ZU FORESCOUT

Forescout ist ein führender Anbieter für Enterprise of Things-Sicherheit und bietet eine ganzheitliche Plattform, die alle vernetzten Geräte in jedem beliebigen heterogenen Netzwerk permanent identifiziert, segmentiert und geltende Vorschriften durchsetzt. Die Forescout-Plattform ist die am häufigsten bereitgestellte und am stärksten skalierbare Enterprise-Lösung für agentenlose Gerätetransparenz und -kontrolle. Sie kann schnell in Ihrer vorhandenen Infrastruktur bereitgestellt werden und erfordert keine Agenten, Upgrades oder 802.1X-Authentifizierung. Fortune 1000-Unternehmen und Behörden vertrauen auf Forescout zur Reduzierung des Risikos von Geschäftsunterbrechungen durch Sicherheitsvorfälle und -verstöße, Gewährleistung und Nachweis von Sicherheitskonformität und Steigerung der Produktivität von Sicherheitsteams.

forescout.com/platform/eyeSight

info-dach@forescout.com

Telefon (weltweit): +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

E-Mail: info-dach@forescout.com
Telefon (weltweit): +1-408-213-3191
Support: +1-708-237-6591

Weitere Informationen finden Sie unter Forescout.de