Checkliste für Angriffsflächen

Die aktuellen Angriffsflächen werden immer größer und komplexer. Mit jedem neuen Cyber-Asset, das in Ihre IT-Umgebung integriert wird, entstehen zugleich neue potenzielle Angriffspunkte.

Diese Checkliste hilft Ihnen dabei, den Schutz Ihrer Angriffsfläche systematisch zu überprüfen: Wo sind Sie bereits gut aufgestellt – und wo könnten sich noch Blindspots, also bislang unentdeckte Risiken, verbergen? Ordnen Sie jedes Element nach folgendem Prinzip ein:

- Bewusste Kenntnis: Cyber-Assets, die Ihnen bekannt sind und die nachweislich Teil Ihrer Angriffsfläche sind.
- Bewusste Unkenntnis: Cyber-Assets, von denen Sie wissen, dass sie zu Ihrer Angriffsfläche gehören, die Sie jedoch möglicherweise nicht aktiv überwachen oder verwalten.
- Unbewusste Unkenntnis: Cyber-Assets, die möglicherweise Teil Ihrer Angriffsfläche sind – oder auch nicht. Sie haben darüber keine gesicherten Informationen.
- n/a: Cyber-Assets, die Sie mit absoluter Sicherheit ausschließen können und definitiv nicht Teil Ihrer Angriffsfläche sind.

Notieren Sie Ihre Antworten in der Checkliste und übertragen Sie sie am Ende auf das Übersichtsblatt auf Seite 11. So erhalten Sie einen kompakten Überblick über Ihre potenzielle Angriffsfläche.

Beachten Sie, dass bestimmte Arten von Assets mehreren Kategorien zugeordnet werden können (z. B. kann ein Gerät sowohl als mobiles Gerät als auch als Endgerät gelten) – und das ist vollkommen in Ordnung! Entscheidend ist eine lückenlose Erfassung, denn jeder eliminierte Blindspot verringert die Angriffsfläche und nimmt Cyberkriminellen die Gelegenheit, sich unbemerkt Zugang zu Ihrer Umgebung zu verschaffen.

Endgeräte

Unternehmensgeräte sowie private Endgeräte der Mitarbeitenden (BYOD), die mit dem Netzwerk verbunden sind. Dazu gehören vor allem Android, ChromeOS-, iOS-, Linux-, Mac- und Windows-Geräte.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Desktop-Computer
- Laptops

Management-Tool(s):

- IT Asset Discovery
- Modern Device Management (MDM)
- Unified Endpoint Management (UEM)

Mobile Geräte

Unternehmens- und private Endgeräte der Mitarbeitenden (BYOD), die in der Regel über Wi-Fi mit dem Netzwerk verbunden sind und für den mobilen Einsatz sowie einfache Transportierbarkeit ausgelegt wurden. Dazu gehören vor allem Android- und iOS-Geräte.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Smartphones
- Smartwatches
- Tablets

Management-Tool(s):

- IT Asset Discovery
- Mobile Device Management (MDM)
- Modern Device Management (MDM)

Robuste Geräte

Mobile Geräte, die speziell dafür entwickelt wurden, extremen Bedingungen standzuhalten – etwa auf Baustellen, in Produktionsstätten oder Lagerhäusern – wo herkömmliche Geräte schnell an ihre Grenzen stoßen würden. Dazu gehören vor allem Android-, iOS- und Windows-Geräte.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Robuste mobile Computer
- Robuste Tablets
- Robuste Wearables

Management-Tool(s):

- IT Assets Discovery
- Mobile Device Management (MDM)
- Modern Device Management (MDM)

Internet of Things (IoT)-Geräte

Nicht standardisierte Endgeräte mit integrierten Sensoren und Software, die über ein Netzwerk oder das öffentliche Internet Daten mit anderen Geräten und Systemen austauschen. Je nach Use Case werden sie auch als Enterprise Internet of Things (eIoT), Extended Internet of Things (XIoT), Industrial Internet of Things (IIoT) oder Internet of Medical Things (IoMT) Geräte bezeichnet.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Geräte für das Asset-Tracking (z. B. RFID-Etiketten)
- Industrielle Sensoren
- Intelligente Geräte (z. B. Toaster, Kühlschränke, Glühlampen)

Management-Tool(s):

- IT Asset Discovery
- Modern Device Management (MDM)
- Speziell entwickelte IoT-Sicherheitstools (unterschiedlich)
- Unified Endpoint Management (UEM)

Cyber-physische Systeme (CPS)

Systeme, die rechnergestützte und physische Ressourcen miteinander verknüpfen und eng koordiniert arbeiten, um ihre Aufgaben auszuführen.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Building Management Systeme (BMS)
- Industrielle Steuerungssysteme (ICS)
- Betriebstechnologie (OT)
- Robotersysteme

Management-Tool(s):

- IT Asset Discovery
- Schutzplattformen für cyber-physische Systeme (CPS)
- Modern Device Management (MDM)

Netzwerkgeräte

Geräte, die die Kommunikation und Interaktion zwischen anderen Geräten in einem Netzwerk unterstützen. Netzwerkgeräte bilden die Netzwerkinfrastruktur.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Router
- Switches
- Firewalls
- Access Points

Management-Tool(s):

- Network Discovery Tools

Server/Rechenzentrumsgeräte

Geräte, die die Verarbeitung, Speicherung und Weitergabe von Daten unterstützen. Sie gelten als das Rückgrat von Diensten wie E-Mail-Kommunikation und Websites.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Server (z. B. E-Mail-Server, Druckserver, Webserver)
- Speichersysteme

Management-Tool(s):

- IT Asset Discovery
- Modern Device Management (MDM)
- Unified Endpoint Management (UEM)

Geräte mit festgelegter Funktion

Geräte, die für spezifische Use Cases entwickelt wurden – oft mit direktem Kundenkontakt.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Kassensysteme (Point-of-Sale-/POS-Systeme)
- Selbstbedienungskioske

Management-Tool(s):

- IT Asset Discovery
- Modern Device Management (MDM)
- Unified Endpoint Management (UEM)

Cloud-Services

Cloud Computing ermöglicht den bedarfsgesteuerten Zugriff auf Computing-Ressourcen über das Internet und wird in verschiedenen Modellen organisiert: Private Cloud (auch als „interne Cloud“ oder „Unternehmens-Cloud“ bezeichnet), Public Cloud, Hybrid Cloud und Multi-Cloud-Umgebungen.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Cloud-Container
- Lösungen für die Datenspeicherung in der Cloud
- Private Cloud mit zugrundeliegenden Rechenressourcen (z. B. CPU und Speicher)
- Public Cloud Services (z. B. AWS, Google Cloud Platform, Microsoft Azure Cloud-Services)

Management-Tool(s):

- Cloud-Native Application Protection Platform (CNAPP)
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP)

Software-as-a-Service (SaaS)-Anwendungen

On-Demand-Anwendungen, die über ein Cloud-Computing-Servicemodell bereitgestellt werden, bei dem der Dienstanbieter die gesamte zugrunde liegende Infrastruktur verwaltet.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Microsoft 365
- Salesforce
- Slack

Management-Tool(s):

- SaaS Security Posture Management (SSPM)

Code

Eine Abfolge von Anweisungen, die in einer Programmiersprache verfasst sind und einem Computer vorgeben, welche Aufgaben er ausführen soll – die grundlegenden Bausteine der Software.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Code für maßgeschneiderte Software, die intern oder für Kunden entwickelt wurde
- Code für proprietäre Software, die für den kommerziellen Vertrieb entwickelt wurde

Management-Tool(s):

- Container-Scanner
- Dynamic Application Security Testing (DAST)
- Mobile Application Security Testing (DAST)
- Open-Source-Software (OSS)-Scanner
- Software Composition Analysis (SCA)
- Static Application Security Testing (SAST)

Commercial Off-the-Shelf (COTS) Software und Anwendungen

Computerprogramme, die von einem Unternehmen erworben und genutzt werden, werden entweder von einem Drittanbieter gekauft oder bereits auf einem Gerät vorinstalliert.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Betriebssysteme (z. B. Windows, macOS, Linux)
- Produktivitäts-Suites (z. B. Microsoft Office)
- Anwendungen von Drittanbietern (z. B. Zoom)

Management-Tool(s):

- IT Asset Discovery
- Patch Management

Internetverbundene Assets

Cyber-Assets, die direkt über das öffentliche Internet zugänglich sind. Diese Assets bilden die sogenannte „externe Angriffsfläche“.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Zertifikate / Domains
- Entwicklungs- und QA-Umgebungen (IP-Adressen)
- Websites (Webserver)

Management-Tool(s):

- External Attack Surface Management (EASM)

Digitale Assets

Eine Kombination aus Assets, wie beispielsweise Daten aus dem Dark Web und sozialen Medien, die zwar nicht als herkömmliche IT-Assets gelten, aber dennoch die Marke, Reputation oder Sicherheit eines Unternehmens gefährden können.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Online-Foren
- Konten in sozialen Medien

Management-Tool(s):

- Digital Risk Protection (DRP)

Identität und Zugriff

„Identität“ bezieht sich auf die digitale Identität einer Person, die mit einem Unternehmen verbunden ist – ihr Name, ihre Berufsbezeichnung, ihr Manager, ihre direkten Vorgesetzten, ihre Telefonnummer und andere derartige Informationen. „Zugriff“ steht für die Ressourcen und Daten, die eine Person aufgrund von Faktoren wie ihrer Berufsbezeichnung oder ihrer Sicherheitsüberprüfung einsehen und/oder bearbeiten darf.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Benutzeridentitäten
- Zugriffsebenen

Management-Tool(s):

- Identitäts- und Zugriffsmanagement (IAM)
- Identitätsanbieter (IdP)

Daten

Daten, die von einem Unternehmen erstellt oder erfasst werden und für Planung, Entscheidungsfindung sowie den täglichen Betrieb genutzt werden.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Kreditkarteninformationen des Kunden
- Geistiges Eigentum (IP)
- Krankenakten der Patienten
- Personenbezogene Daten (PII) (z. B. Kundenkontaktdaten)

Management-Tool(s):

- Schutz vor Datenverlust (DLP)
- Data Security Posture Management (DSPM)

Application Programming Interfaces (APIs)

Sätze von Regeln und Protokollen, die es verschiedenen Softwareanwendungen ermöglichen, miteinander zu kommunizieren.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- HubSpot-APIs
- Salesforce-APIs
- Slack-APIs

Management-Tool(s):

- API-Schutzprodukte
- API Security Posture Tools

Drittanbieter-Assets

Moderne Unternehmen arbeiten oft mit mehreren externen Partnern zusammen und teilen dabei Systeme und Daten, um Geschäftsprozesse zu optimieren und die Effizienz zu steigern. Doch je enger zwei Unternehmen miteinander vernetzt sind, desto größer wird auch ihre gemeinsame Angriffsfläche.

Bewusste Kenntnis	☐
Bewusste Unkenntnis	☐
Unbewusste Unkenntnis	☐
n/a	☐

Beispiele:

- Website des Wiederverkaufspartners
- Cloud-Infrastruktur der Marketingagentur
- Die Entwicklungsumgebung des Lieferkettenpartners

Management-Tool(s):

- External Attack Surface Management (EASM)

	Sichtbarkeit			
Asset-Kategorie	Bewusste Kenntnis	Bewusste Unkenntnis	Unbewusste Unkenntnis	n/a
Endgeräte	☐	☐	☐	☐
Mobile Geräte	☐	☐	☐	☐
Robuste Geräte	☐	☐	☐	☐
Internet of Things (IoT)-Geräte	☐	☐	☐	☐
Cyber-physische Systeme (CPS)	☐	☐	☐	☐
Netzwerkgeräte	☐	☐	☐	☐
Server / Rechenzentrumsgeräte	☐	☐	☐	☐
Geräte mit festgelegter Funktion	☐	☐	☐	☐
Cloud-Services	☐	☐	☐	☐
Software-as-a-Service (SaaS)-Anwendungen	☐	☐	☐	☐
Code	☐	☐	☐	☐
Commercial Off-the-Shelf (COTS) Software und Anwendungen	☐	☐	☐	☐
Internetverbundene Assets	☐	☐	☐	☐
Digitale Assets	☐	☐	☐	☐
Identität und Zugriff	☐	☐	☐	☐
Daten	☐	☐	☐	☐
Application Programming Interfaces (APIs)	☐	☐	☐	☐
Beziehungen zu Drittanbietern	☐	☐	☐	☐

Über Ivanti

Ivanti baut die Barrieren zwischen IT und Sicherheit ab, damit Everywhere Work erfolgreich ist. Ivanti hat die erste eigens entwickelte Technologieplattform für CIOs und CISOs geschaffen, die IT- und Sicherheitsteams umfassende Softwarelösungen bietet. Diese skalieren mit den Anforderungen ihrer Unternehmen, um die positiven digitalen Erfahrungen der Mitarbeitenden zu ermöglichen, zu sichern und zu verbessern. Die Ivanti-Plattform wird von Ivanti Neurons betrieben – einer intelligenten, Cloud-fähigen Hyper-Automatisierungsebene, die eine proaktive Fehlerbehebung ermöglicht, benutzerfreundliche Sicherheit im gesamten Unternehmen bietet und ein herausragendes Mitarbeitererlebnis schafft. Mehr als 35.000 Kunden, darunter 85 der Fortune-100-Unternehmen, haben sich für Ivanti entschieden, um die Herausforderungen mit den eigenen End-to-End-Lösungen zu meistern. Unser Ziel bei Ivanti ist, ein Umfeld zu schaffen, in dem alle Meinungen gehört, respektiert und geschätzt werden. Und wir setzen uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeitenden und unseren Planeten ein. Weitere Informationen finden Sie unter ivanti.com und folgen Sie @GoIvanti.

ivanti

Für weitere Informationen oder um Ivanti zu kontaktieren, besuchen Sie bitte ivanti.com.