Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

EASM

External Attack Surface Management

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten,** regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

Was wir dabei oft vergessen, sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

EASM – Was ist das?

External Attack Surface Management (EASM) ist ein Ansatz in der Cybersicherheit, der darauf abzielt, die **Angriffsfläche einer Organisation**, die von außen sichtbar ist, **systematisch zu identifizieren**, zu **überwachen** und zu **minimieren**. Dabei handelt es sich um alle Systeme, Netzwerke und Technologien, die öffentlich zugänglich sind und daher potenzielle Ziele für Cyberangriffe darstellen könnten. Dies kann Webanwendungen, Cloud-Dienste, Netzwerkendpunkte, offene Ports, veraltete Software und vieles mehr umfassen.

Das Hauptziel von EASM ist die **frühzeitige Erkennung** von **Schwachstellen** und **Sicherheitsrisiken**, um präventive Maßnahmen ergreifen zu können, bevor ein Angriff stattfindet. Einmal identifizierte und klassifizierte Risiken können dann priorisiert werden, um entsprechende **Abwehrmaßnahmen** zu ergreifen.

Wer sollte EASM nutzen?

Grundsätzlich kann **jede Organisation, die eine Online-Präsenz hat** oder **vernetzte Systeme** nutzt, von External Attack Surface Management (EASM) profitieren. Einen besonderen Fokus sollten Unternehmen auf EASM legen, die eines oder mehrere dieser Kriterien erfüllen:

- Unternehmen mit einer **großen** oder **komplexen Infrastruktur** die eine Vielzahl von Anwendungen und Systemen enthält
- Unternehmen, die Marken oder Domains haben, die gerne für **Cybersquatting oder Phishing-Angriffe** gegen Mitarbeiter oder Kunden verwendet werden
- Unternehmen, die **Fusionen und Akquisitionen** durchführen, um einen Überblick über Problembereiche oder übersehene Bestandteile zu bekommen
- Unternehmen, die sichergehen wollen, dass alle Internetauftritte mit entsprechenden und **gültigen SSL-Zertifikaten** geschützt sind und diese Auftritte auch den gängigen Cookie-Vorgaben der **DSGVO** entsprechen
- Unternehmen, die sich nicht sicher sind, ob sie alle Assets auch wirklich im Blick haben, oder ob nicht doch eine Abteilung ohne Rücksprache mit der IT **Schatten-IT (Shadow-IT)** aktiv betreibt
- Unternehmen, die verifizieren möchten, dass die Assets, die von außen erreichbar sind, auch richtig konfiguriert wurden
- Unternehmen, die sicher gehen wollen, dass sie **alle Assets im Blick** und wartbar haben, um für Angreifer auf der Suche nach neuen Zielen so unattraktiv wie möglich zu sein

Cyber-Sicherheitsrat Deutschland e.V.

Welche Maßnahmen sind erforderlich?

Für die Umsetzung von EASM müssen Unternehmen initial einen **Ausgangspunkt** für die Scans festlegen. Das kann eine Domain oder auch nur eine IP-Adresse sein. Danach ist es nötig, dass weitere Funde von Lookalikes oder möglichen weiteren Assets zum Scope hinzugefügt oder ausgeschlossen werden.

Es ist jedoch nicht nur damit getan, dass man die Ergebnisse überwacht und regelmäßig den Scope erweitert, um sicherzustellen, dass man weiterhin die **komplette Angriffsfläche im Blick** behält. Man muss auch **Prozesse** festlegen, wie man mit **gefundenen Schwachstellen** und Assets umgeht. Wer kümmert sich um die Patches? Wie ermittelt man die Kontaktpersonen bei Shadow-IT oder Assets, die man vorher nicht im Blick hatte oder für die man nicht zuständig ist? Wie fragmentiert ist die IT-Security im Unternehmen und wie einfach kommunizieren die Ticket-Systeme oder Ansprechpartner untereinander? Welche Workflows werden befolgt, um die gefundenen Schwachstellen zu beheben?

Ergänzend dazu ist es oftmals nicht nur mit der Symptombekämpfung getan. Je nachdem welche Erkenntnisse durch EASM gewonnen werden, muss man möglicherweise andere Bereiche wie **interne Schulungen, Richtlinien für IT-Assets oder Verwaltungsworkflows** in Frage stellen und überarbeiten.

Erwähnenswert ist auch, dass EASM kein einmaliges Projekt ist. EASM ist ein **fortlaufender Prozess**, der darauf aufbaut, dass Sicherheitsverantwortliche ständig Ergebnisse analysieren, bewerten, beheben und dann erneut auditieren. So kann man den **Status und die Größe der Angriffsfläche** über die Zeit hinweg verbessern und verkleinern, um sich so unattraktiv wie möglich für potenzielle Angreifer zu machen.

Welche Chancen gibt es?

EASM bietet eine Reihe von Vorteilen und Chancen für IT-Verantwortliche:

- EASM gibt einen Einblick in den **aktuellen Status-Quo** der Assets, die über das Internet erreichbar sind.
- EASM hilft dabei, bekannte und unbekannte Assets zu inventarisieren und zu kategorisieren.
- EASM zeigt auf, wo mögliche **Verstöße gegen Cookie-Richtlinien** oder **SSL-Best-Practices** vorhanden sind, die möglicherweise Interessenten abschrecken.
- EASM gibt einen ersten **Überblick über die Sicherheitslage** dieser Assets und zeigt an, wo möglicherweise schneller **Handlungsbedarf** nötig ist, um kritische Sicherheitslücken zu schließen.

- EASM bietet die Möglichkeit, Assets und Domains aufzuspüren, die möglicherweise dem Unternehmensruf schaden oder für **Cyberangriffe** missbraucht werden können.
- EASM zeigt **Abhängigkeiten** der **Web-Infrastruktur** untereinander auf und hilft so dabei, Auswirkungen oder Konsequenzen von Änderungen besser einzuschätzen.
- EASM und das darin enthaltene dynamische Inventar der extern erreichbaren Assets hilft dabei, **fundierte Entscheidungen** über **Investitionen** und **Sicherheitsstrategie** zu treffen.
- EASM ist nützlich, um Annahmen über die Effektivität der Sicherheitsmaßnahmen einem ersten **Reality-Check** zu unterziehen. Sind alle Assets bekannt? Sind diese auch richtig konfiguriert? Wurden alle Ports - soweit nötig - geschlossen? Hält sich jeder Mitarbeiter an die **IT-Richtlinien**? Ist nur das sichtbar und erreichbar, was gesehen und erreicht werden soll?

Welche Risiken gibt es?

Obwohl EASM-Lösungen oftmals sehr leistungsfähig sind, gibt es dennoch einige Risiken, die erwähnt werden sollten:

Aufgrund der Natur der Dinge werden EASM-Tools mitunter wahrscheinlich falsche oder **unzutreffende Alarme** auslösen, da eine Attack Surface Management-Lösung nicht die gleiche Tiefe wie ein manueller Pentest hat.

Durch die Vorgehensweise bei der Implementierung kann es eine gewisse Zeit dauern, ehe die Scanner alle möglichen und potenziellen Domains, IP-Adressen und Assets gefunden haben, die zur Organisation gehören. Um Lookalikes oder **Fakes zu identifizieren**, ist es nötig, regelmäßig den **Scope der Scans zu überprüfen** und bei Bedarf weitere Assets mit in die Analysen einzubinden. Nur so kann man die **dynamische Angriffsfläche im Blick behalten** und mögliche **Sicherheitsrisiken** rechtzeitig entdecken.

Das beste Tool hilft nichts, wenn man mit den Ergebnissen dann nichts anfängt. Das gilt auch für EASM-Lösungen. Daher ist es wichtig, dass man bestehende Prozesse erweitert, um die **Ergebnisse von EASM an die passenden Verantwortlichen zu leiten**, oder bei der Implementierung der Lösung Prozesse definiert, wie man damit umgeht.

EASM ist ein Prozess und **kein One-Off Projekt**. Das bedeutet auch, dass Manpower und Zeit für eine tatsächliche Verbesserung der Sicherheitslage benötigt werden. Wenn niemand Zeit hat, die Ergebnisse und neue potenzielle Matches zu prüfen, dann ist es nur ein weiteres Tool im Tech-Stack, „das man sich mal genauer anschauen sollte".

Fazit

EASM ist eine wirkungsvolle Lösung, um sich ein Lagebild über die externe **Angriffsfläche einer Organisation** zu verschaffen. Es bietet nicht nur die Möglichkeit, **Risiken und Schwachstellen extern erreichbarer Assets** systematisch zu identifizieren und zu inventarisieren, sondern liefert auch wertvolle Daten für strategische Entscheidungen. Jedoch ist es nicht damit getan, einmalig einen solchen Scan laufen zu lassen, sondern erfordert eine **kontinuierliche Pflege** und **Analyse** der Funde. Obwohl die erste Implementierung und das Scoping bei größeren Organisationen durchaus Zeit in Anspruch nehmen, sollte man sich nicht davon abschrecken lassen.