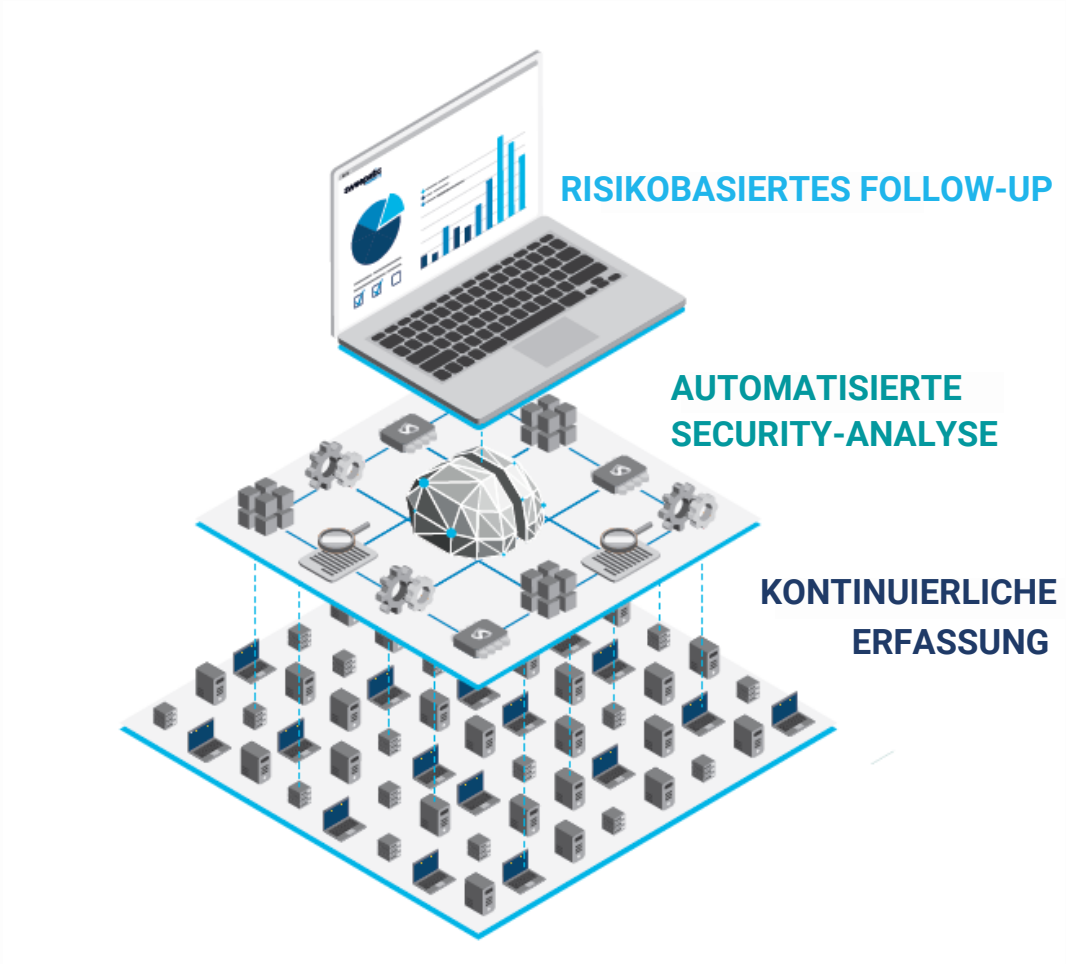
sweepatic SECURITY

External Attack Surface Management: Key Features

WHITE PAPER

APRIL 2021
Update: März 2022



Was ist ein External Attack Surface Management?

Seit einigen Jahren gibt es einen neuen Bereich für Cybersecurity-Lösungen mit einer eigenen Definition: Attack Surface Management oder ASM. Gartner, Forrester und andere Branchenanalysten haben den Begriff in jüngsten Berichten beschrieben und das Wort „extern" hinzugefügt, um die Outside-in-Perspektive dieser Lösungen zu verdeutlichen. Der Begriff External Attack Surface Management kann jedoch verwirrend oder vage sein, wenn man sich nicht etwas Zeit für eine klare Definition nimmt. Im Bereich der Cybersecurity gibt es viele Angriffsflächen, die zum Ziel von Hackern werden können. Von welcher Oberfläche sprechen wir also?

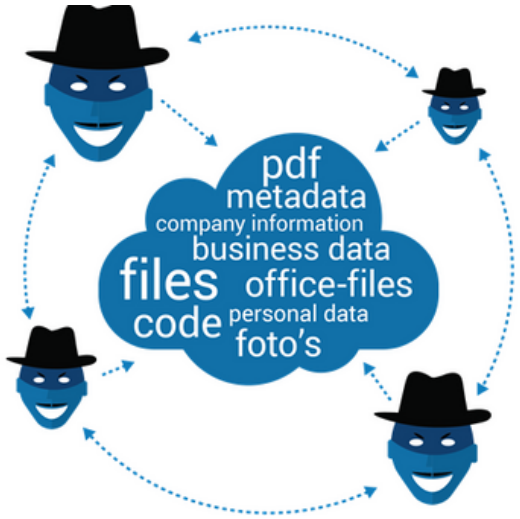
> *In der Cybersecurity wird das Wort Angriffsfläche für öffentlich oder extern verfügbare oder mit dem Internet verbundene IT-Assets verwendet.*

Attack Surface Management kann also auch mit Securitymanagement der Internet-exponierten IT-Assets übersetzt werden. Da dies zu lang ist und schnell kompliziert klingt, haben wir es einfach mit ASM abgekürzt.

IT-Assets können – außerhalb ihrer „normalen" Funktion – alles das sein, was einem Angreifer normalerweise helfen kann, relevante Informationen zu erhalten, um einen Angriff zu starten. Assets können sein: IP-Adressen, DNS-Records, Anwendungsendpunkte, Webseiten, APIs, (administrative) Remote-Zugriffspunkte, Datenbanken, Verschlüsselungsdetails, File-Sharing-Services, gestohlene Anmeldedaten, die im Dark Web verkauft werden, usw. Das Endziel ist in der Regel, Schwachstellen, unsichere Konfigurationen, Daten oder andere Probleme zu finden, die missbraucht werden können.

Warum ist eine aufgeräumte Angriffsfläche wichtig?

Ein Angreifer wird so viele Informationen und Schwachstellen wie möglich finden, um die beste Angriffsstrategie zu entwickeln. Er wird normalen Datenverkehr und Suchanfragen simulieren, um so viele Daten wie möglich zu sammeln. Je sauberer Ihre Angriffsfläche ist, desto mehr Mühe muss er sich geben. Dies kann dazu führen, dass der Angreifer zu einem leichteren Ziel weiterzieht.



> *Attack Surface Management ist die Kunst, für Cyberkriminelle so unattraktiv wie möglich zu werden.*

Warum sind Attack Surface Management-Tools so wertvoll?

Die Angriffsfläche von Unternehmen und Organisationen wird immer komplexer. Grund dafür sind einige wichtige Trends wie:

- der kontinuierliche Fokus auf die **Digitalisierung**, um wettbewerbsfähig zu bleiben;
- die **Umstellung auf die Cloud** und die Geschwindigkeit der Bereitstellung durch die Cloud;
- die **Multi-Cloud-Ansätze**, die viele Unternehmen zur Optimierung verfolgen;
- die **Befähigung von Nicht-IT-Mitarbeitern**, Anwendungen online über SaaS-Angebote zu nutzen;
- eine **Belegschaft, die immer mobiler ist**, da sie sich von überall verbinden und jedes Gerät nutzen kann;
- **Cybersecurity-Experten**, deren Zeit nur begrenzt ist und die teuer und schwer zu finden sind;
- die **ständige Weiterentwicklung von Online-Assets**, durch die halbjährliche Schwachstellen-Scans oder andere technische Cybersecurity-Assessments aus Risikosicht viel zu langsam und selten sind.

Für Unternehmen wird es also immer schwieriger, den Überblick darüber zu behalten, welche IT-Assets online verfügbar sind, und den kontinuierlichen Strom neu bereitgestellter Assets zu verfolgen – sowohl On-Premises als auch in diversen Clouds. Die größten Herausforderungen liegen oft in mittleren bis großen Unternehmen. Diese verwalten einen Mix aus alter und neuer IT-Infrastruktur, die kontinuierlich angepasst und aufgerüstet wird. Vor allem große Unternehmen haben oft verschiedene Untermarken mit eigenen IT-Teams und Mandaten.

Unternehmenscluster, Marken oder Abteilungen ziehen es vor, bei dem Thema Security zusammenzuarbeiten, anstatt in ihren eigenen Silos in Personal und Tools zu investieren. In vielen Fällen wird ein CISO oder ein Security-Team mit der Aufgabe betraut, die Security in der gesamten Holding oder im gesamten Unternehmen zu verbessern. Doch eine der großen Herausforderungen besteht darin, alle mit dem Internet verbundenen IT-Assets zu kennen.

Gespräche mit den verschiedenen Teams zu führen, dauert oft zu lange, ist zu komplex und führt zu unvollständigen und nur schwer nachvollziehbaren Ergebnissen. In diesen Fällen wäre eine Lösung, die die IT-Assets automatisiert und kontinuierlich erkennt, sehr wertvoll.

Was sind die häufigsten Anwendungsfälle für die Einführung einer EASM-Lösung?

Unternehmen ziehen eine EASM-Lösung aus verschiedenen Gründen in Betracht. Die Reduzierung der Angriffsfläche ist eine wichtige Taktik für die Cybersecurity. Andere häufige Gründe sind:

- Erkennen von **unbekannten und nicht verwalteten Assets**, Schatten-IT und Schattenprojekten in der Infrastruktur vor Ort und in Clouds.
- Auffinden von **Schwachstellen und Risiken**, die von herkömmlichen Schwachstellenscannern nicht entdeckt werden.
- **Reduzierung der Angriffsfläche für das Internet**: Was nicht online ist, kann nicht gehackt werden. So einfach ist das.
- Bewertung der Risiken von **Lieferanten und IT-Anbietern**.
- Bewertung von **Fusions- und Übernahmezielen** und Risiken von Tochtergesellschaften.
- Erkennung von **externen Risiken** durch Daten, die außerhalb der Infrastruktur des Unternehmens gehostet werden, wie die gestohlenen Anmeldeinformationen im Dark Web und von Cybersquatting-Aktivitäten, die die Marke missbrauchen.
- **Zeitersparnis und Einsparung teurer Cybersecurity-Ressourcen** durch Automatisierung der manuellen Arbeit, die beim Zusammenfügen von Erkenntnissen aus frei verfügbaren Open-Source-Scan-Tools (OSINT) erforderlich ist.
- **Kooperation bei der Security**: Eine externe Lösung zur Verwaltung von Angriffsflächen bietet einen abteilungs- und markenübergreifenden Security-Überblick. Verschiedene Profile können auf die Plattform zugreifen, um die benötigten Informationen zu erhalten und die Risiken in ihrem Bereich zu verfolgen. Jeder sieht die Ergebnisse, sowohl die von ihm selbst als auch die von anderen ergriffenen Maßnahmen, was alle für das gemeinsame Ziel motivieren kann. Die Geschäftsleitung kann die wichtigsten Kennzahlen leicht nachverfolgen.

Was ist der Unterschied zwischen einem externen Angriffsflächen-Scanner und einem Schwachstellen-Scanner?

Viele fragen sich, wie sich ein EASM-Scanner von einem herkömmlichen Schwachstellen-Scanner unterscheidet. Im Folgenden sind einige Beispiele aufgeführt.

1. **Nur für das Internet:** Eine EASM-Lösung ist auf die Erkennung von Risiken im Internet spezialisiert.

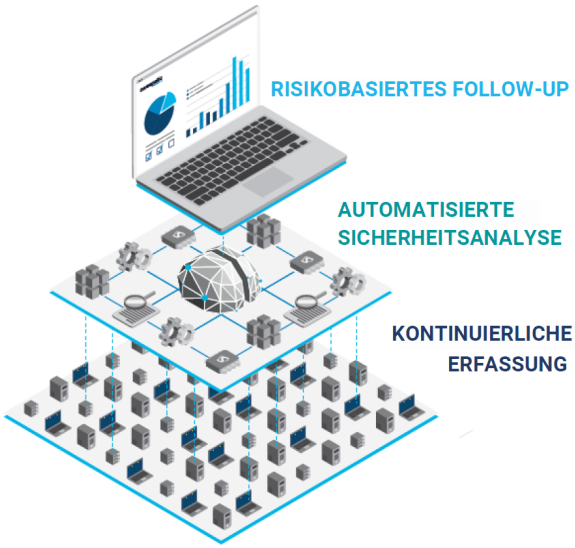
2. **Entdeckt Unbekanntes:** Ein Schwachstellen-Scanner konzentriert sich auf bekannte Assets, indem er von einer Liste bekannter IP-Adressen oder bekannter Cloud-Provider ausgeht. EASM-Scanner sind auf die Erkennung von bekannten und unbekannten Assets auf der Grundlage von DNS-Informationen und nicht von IP-Adressen spezialisiert. Sie benötigen nicht viele Eingaben, um loszulegen.

3 **Bewertet mehr als nur Softwareschwachstellen:** Ein Schwachstellen-Scanner sucht nur nach Software-Schwachstellen und ist ein Experte darin, sie alle zu finden. Die Scans können sogar in einen echten Angriffsmodus übergehen, je nachdem, wie aggressiv der Scan ausgeführt wird. Damit automatisiert er einen Teil der manuellen Arbeit eines Pen-Testers. Bei der Verwendung aggressiver Scans ist Vorsicht geboten, da sie Systeme beschädigen oder sogar zum Absturz bringen können.

Eine externe Angriffsflächenlösung simuliert den normalen Internetverkehr und ist standardmäßig sicher in der Anwendung. Sie findet mehr als nur Software-Schwachstellen. Sie kann IP-Adressen entdecken, die bisher unbekannt waren, so dass sie in die Liste der Schwachstellen-Scanner aufgenommen werden können.

Was sind die wichtigsten Merkmale einer Plattform zur Verwaltung externer Angriffsflächen?

EASM unterstützt Cybersecurity-Experten, indem es ihnen einen Großteil der schweren manuellen Arbeit abnimmt, so dass sie sich auf die tatsächliche Lösung der Probleme konzentrieren können, anstatt sie zu finden.



Technisch versierte Fachleute wissen, wie man die breite Palette verfügbarer Open-Source-Scan-Tools und Security-Test-Skripte einsetzt, aber die Korrelation und Speicherung aller zurückgegebenen Daten und Schlussfolgerungen ist keine einfache Sache. Eine EASM-Plattform ist stark automatisiert und sollte leicht einzurichten und in Betrieb zu nehmen sein.

Eine EASM-Lösung hat in der Regel drei Hauptmerkmale:

- Kontinuierliche Erfassung
- Automatisierte Security-Analyse
- Risikobasiertes Follow-up

1 **Kontinuierliche Erfassung**

Der Zweck der EASM-Lösung besteht darin, die Ermittlung Ihrer Bestände zu automatisieren. Sie sollte auf der Grundlage Ihrer primären Domäne (z.B. mycompany.com) oder einer Liste von primären Domänen für größere Organisationen gestartet werden können. Es sollte nicht nötig sein, IP-Adressen anzugeben, um loszulegen.

Das Hinzufügen zusätzlicher IP-Bereiche sollte jedoch für spezielle Anwendungsfälle unterstützt werden, bei denen die Erkennungstechniken nicht weiterhelfen können. Eine EASM-Lösung verwendet einen intelligenten Suchalgorithmus, um mit minimalen Eingaben und einer begrenzten Anzahl von Fehlalarmen eine Übersicht über Ihre Assets zu erstellen.

Der Erkennungsprozess ist fortlaufend, und bei jedem Scan werden Assets gefunden, die neue Scans auslösen. Da es sich um einen kontinuierlichen Prozess handelt, werden wöchentlich neu installierte oder entfernte Assets erkannt und gemeldet.

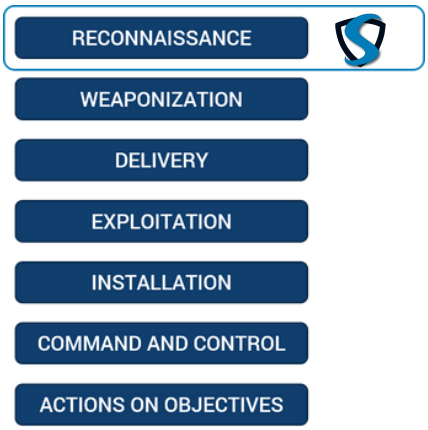
Typische Elemente der Assets, die entdeckt werden sollen:

- Alle DNS-Einträge
- Alle zugehörigen IP-Adressen
- WHOIS- oder DNS-Registrierungsinformationen
- Geo-Standorte der Assets
- Für die Assets zuständige Hosting-Provider
- Alle offenen Ports
- Alle verwendeten SSL/TLS-Zertifikate und deren Details
- E-Mail-Systeme
- DNS-Systeme
- Anwendungen wie Websites, E-Mails, DBs, Fernzugriff, Dateifreigaben usw.
- Softwareversionen, die in den ermittelten Assets und Anwendungen verwendet werden
- Login-Seiten

2

Automatisierte Security-Analyse

Auf der Grundlage der Ergebnisse werden weitere Überprüfungen durchgeführt, um festzustellen, wo Security-Probleme gefunden werden können.



Source: SANS, Cyber Kill Chain

Wie von SANS Security Awareness erläutert, umfasst das Cyber-Kill-Chain-Modell sieben Schritte, die ein Angriff durchläuft. Jeder Angriff beginnt mit einer Aufklärungsphase. Hacker betreiben heute gut organisierte kriminelle Unternehmen, die stark automatisiert sind und über die besten Tools verfügen. Wenn Sie sich nicht selbst automatisieren, kämpfen Sie einen ungleichen Kampf.

Typische Security-Probleme, die gefunden werden können:

- Software-Schwachstellen auf der Grundlage der entdeckten Software-Versionsinformationen
- Unsichere E-Mail-Konfigurationseinstellungen, wie fehlende oder falsche SPF-, DMARC- und DKIM-Einstellungen
- Schwache Verschlüsselung, wie die Verwendung sehr alter und unsicherer SSL/TLS-Verschlüsselungsprotokolle
- Ungesicherte DNS-Einrichtungen, die DNS SEC nicht unterstützen
- Standardinstallationen, wie ein Webserver, der nach der Erstinstallation eine Standardseite anzeigt
- Fehlercodes, wie HTTP-Antwortfehler, ein Hinweis auf eine falsch konfigurierte oder veraltete Website
- IP-Blacklisting und Reputationsprobleme
- Unverschlüsselte Anmeldeseiten, die zum Diebstahl von Passwörtern führen
- Unnötig exponierte Services, wie Datenbanken und gefährliche Fernverwaltungsprotokolle (z.B. Telnet, RDP & VNC)
- Gestohlene Anmeldedaten: Warnungen auf der Grundlage kürzlich bekannt gewordener gestohlener Anmeldedaten für Ihr Unternehmen
- Phishing & Cybersquatting-Websites, d.h. ähnliche Websites, die Ihre Marke missbrauchen

3 **Risikobasiertes Follow-up**

Eine EASM-Lösung priorisiert die gefundenen Probleme sofort mit einer integrierten risikobasierten Engine. Dies ist ein hervorragender erster Schritt für jedes Unternehmen.

Das erste Ziel besteht darin, die größten Probleme in Ihrer Infrastruktur zu beheben. Es ist wichtig, große Lücken in weniger wichtigen Systemen zu beheben, da sich Hacker auf diese konzentrieren, um einen Fuß in die Tür zu bekommen, und sich dann seitlich zu den wirklich interessanten Produktionssystemen und Daten bewegen. Genau das passiert bei einem Ransomware-Angriff, bei dem ein schwaches System/ein schwacher Benutzer gehackt wird, woraufhin viele andere Assets folgen.

Nicht alle Assets haben den gleichen Wert für ein Unternehmen. Unternehmen, die die großen Probleme in allen Systemen behoben haben, können ihre Warnungen weiter priorisieren, indem sie sie ihren Prioritäten entsprechend markieren oder sortieren.

> *Eine EASM-Lösung liefert in der Regel eine Risikobewertung und eine Trendlinie im Zeitverlauf, so dass das Management die Entwicklung der geleisteten Arbeit und des verbleibenden Risikos verfolgen kann.*

Da die Ressourcen immer begrenzt sind, werden sich die meisten Unternehmen wahrscheinlich auf eine akzeptable Restrisikopunktzahl einigen. Im Idealfall kann das Unternehmen sehen, wie es im Vergleich zum Durchschnitt seiner Branche abschneidet, der von anderen Unternehmen, die ebenfalls auf der Plattform vertreten sind, ermittelt wurde.

Sweepatic ist eine External Attack Surface Management-Lösung

Unsere Kunden nutzen die Erkennungsfunktion der Sweepatic-Plattform, um **kontinuierlich bekannte und unbekannte IT-Assets** zu finden. Darüber hinaus nutzen sie unsere Plattform, um eine nach **Prioritäten geordnete Liste der entdeckten Security-Probleme** weiterzuverfolgen.

Zusätzlich zu unserer leistungsstarken Erkennungs-Engine untersuchen wir automatisch **Security-Probleme** wie Schwachstellen, Fehlkonfigurationen in E-Mail/DNS/Web, schwache Verschlüsselung, abgelaufene und schwache SSL-Zertifikate, ungeschützte Datenbanken und Dateifreigaben, ungeschützten administrativen Zugriff und vieles mehr und erstellen entsprechende Berichte.

Um eine **persönliche Vorführung** mit einem unserer Sweepatic-Experten zu vereinbaren, besuchen Sie unsere Website oder kontaktieren Sie uns über info@sweepatic.com.