*/ Wir beobachten täglich, wie die Entwicklung der Digitalisierung von Prozessen in unserer Gesellschaft und im Business-Alltag an Fahrt aufnimmt. Dabei werden Dinge schnell online veröffentlicht oder geteilt. Gerade mittlere und größere Unternehmen haben das Problem, sich hier schnell einen Überblick zu verschaffen.

Attack Surface Management für präventive Security-Konzepte

Cyberkriminellen die Basis nehmen

Ein geeignetes ASM verschafft Unternehmen einen vollständigen Überblick der erreichbaren Webseiten, Technologien, IT-Systeme, Internetdienste und Portale mit allen erforderlichen technischen Details. Es läuft vollautomatisch und fortlaufend ab, so dass sehr schnell Maßnahmen ergriffen werden können. Dadurch verlieren Cyberkriminelle die Lust, ihre Spurensuche fortzusetzen, da sie keine Angriffsflächen finden.

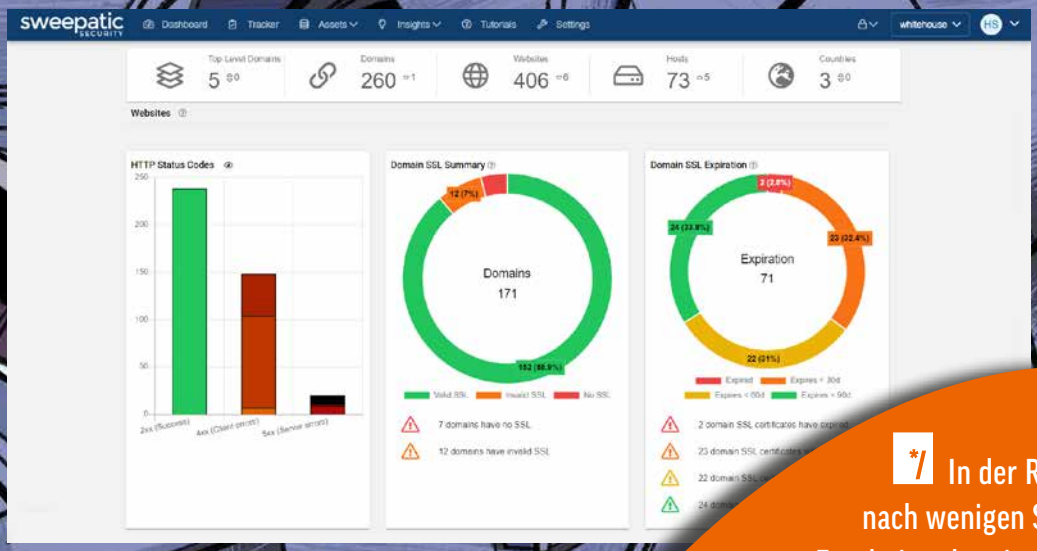
Immer öfter kann man in den Medien verfolgen, dass die Angriffe durch Hacker stark zugenommen haben. Um Attacken planen und durchführen zu können, benötigen diese Kriminellen entsprechende Einfallstore, die den Zugang zu IT-Infrastruktur und -Systemen ermöglicht. Oft hört man in diesem Zusammenhang von Penetrations- oder Vulnerability-Tests als geeigneten Maßnahmen, um Schwachstellen zu erkennen und die Sicherheit gewährleisten zu können. Doch kann es schon viel zu spät sein, wenn diese Verfahren zum Einsatz kommen. Unternehmen bieten heute viele direkte Angriffspunkte über das Internet, die den Hacker dann schlimmstenfalls zu nicht aktualisierten und anfälligen Systemen führen. Mit einem Attack Surface Management (ASM) erhält man zu jeder Zeit ein aktuelles Bild über die eigenen Angriffsflächen mit allen erforderlichen technischen Details und kann sofort geeignete Maßnahmen einleiten.

Gerade in mittelständischen und größeren Unternehmen führt der zunehmende Digitalisierungsgrad von Arbeitsabläufen und Prozessen dazu, dass das Wachstum der Infrastrukturen schnell voranschreitet. Das Ergebnis sind komplexe Vernetzungsstrukturen, die sich zudem auch noch über mehrere Standorte verteilen. Das Dilemma dabei ist einerseits, dass das Management teilweise gar nicht weiß, welchen Sicherheitsrisiken sich das Unternehmen damit täglich über das Internet aussetzt. Andererseits fehlt den Netzwerkverantwortlichen häufig der Überblick hinsichtlich möglicher Einfallstore über das World Wide Web, um durch geeignete Maßnahmen Angriffen den Riegel vorzuschieben.

Security beginnt mit dem richtigen Überblick. »Wir beobachten täglich, wie die Entwicklung der Digitalisierung von Prozessen in unserer Gesellschaft und im Business-Alltag an Fahrt aufnimmt. Dabei werden Dinge schnell online veröffentlicht oder geteilt. Ein weiterer Treiber in diesem Zusammenhang ist die Verlagerung vieler Aktivitäten in die Cloud, die so einfach per Klick den Zugriff auf oder den Abruf von Diensten ermöglicht. Gerade mittlere und größere Unternehmen haben das Problem, sich hier schnell einen Überblick zu verschaffen beziehungsweise diesen auch zu behalten. Mit einer Attack-Surface-Management-Plattform, die praktisch über eine »Suchmaschine« verfügt, die in der Lage ist, alle möglichen, öffentlich erreichbaren Schwachstellen detailliert für eine Analyse zu erfassen, bekommt man das Problem schnell in den Griff«, sagt Stijn Vande Casteele, Founder und CEO von Sweepatic.

Verfügt man über diese Informationen, lassen sich umgehend Maßnahmen ergreifen, die Sicherheitsrisiken ausräumen. Alle IP-Adressen, (Sub-)Domains und Anwendungen, die mit einem Unternehmen in Verbindung stehen, sind so aufzufinden und können übersichtlich dargestellt werden. Häufig erlebt man die Überraschung von Verantwortlichen in Organisationen und Unternehmen über die Ergebnisse, die sie in dieser Form auf einen Blick vorher nicht zur Verfügung hatten. Dabei kommt es oft vor, dass digitale Bereiche entdeckt oder wiederentdeckt werden, die gar nicht mehr auf dem Radar sind. Ein Attack Surface Management einzuführen bedeutet, einen vollständigen Überblick über alle erreichbaren Webseiten, Technologien, IT-Systeme, Internetdienste und Portale zu haben, damit sie alle ordnungsgemäß und sicher überwacht werden können.

Angriffsfläche verringern und Lücken nachhaltig schließen. Anhand von technischen Scans auf der Basis speziell entwickelter Algorithmen sind ASM-Lösungen in der Lage, alle IT-Umgebungen zu erfassen, in die Cyberkriminelle leicht einbrechen können. Dabei zeigt die Darstellung der durchge-



Dashboard Attack Surface Management Plattform

> In der Regel stehen schon nach wenigen Stunden verwertbare Ergebnisse bereit, die sofort in das aktuelle Risiko-Management und die IT-Security-Maßnahmen einbezogen werden können.

führten Analysen die Bereiche geordnet nach Gefährdungspotenzial und Risiko an.

Im Prinzip nimmt das Tool den gleichen Weg wie ein Hacker, um dann die Sicht aus dieser Perspektive übersichtlich abzubilden. Dabei muss das Unternehmen keinen zusätzlichen Input zur Verfügung stellen. Über die offiziellen Domains startet die ASM-Lösung mit den Analysen und entdeckt so typischerweise ungenutzte Domains oder veraltete IT-Umgebungen. Vernachlässigte IT-Ressourcen werden oft nicht aktualisiert und sind das Einfallstor für Kriminelle. Ist diese Hürde erst einmal überwunden, dann ist der Weg frei, tiefer in die Systeme vorzudringen. Was ist also zu tun? Am besten nimmt man alle Ressourcen vom Netz, die nicht gebraucht werden, um die Angriffsfläche zu verringern, und sorgt dafür, dass Zertifikate und Systeme immer auf aktuellstem Stand sind.

Behutsame Scans und priorisierte Sicherheitswarnungen. Eine Sicherheitsbewertung wird für alles durchgeführt, was durch die ASM-Lösung erfasst wurde. Täglich durchgeführte Untersuchungen und Tests prüfen, ob Abweichungen in Bezug auf bestimmte Sicherheitsvorschriften oder Best-Practice-Vorgaben vorliegen. Auch Updates und Konfigurationen können so unter die Lupe genommen werden. Dabei ist es wichtig, dass die Scans und Sicherheitsüberprüfungen behutsam ausgeführt werden, damit sie nicht zu Sicherheitsmeldungen führen oder es Auswirkungen auf laufende Anwendungen gibt, weil außergewöhnlicher Traffic festgestellt wurde. Die Ergebnisse stehen dem Unternehmen anschließend strukturiert und priorisiert nach Risiko zur Verfügung. Es ist nicht das Ziel, eine große Menge an Daten zu liefern, sondern mit einem Tool die essenziellen Daten zu erfassen, die dabei unterstützen, die richtigen und wichtigen Entscheidungen treffen zu können.

Spurensuche stoppen – Angriffe verhindern. Nach Erstellung eines Kontos können die Verantwortlichen direkt mit der Analyse beginnen. In der Regel stehen schon nach wenigen Stunden verwertbare Ergebnisse bereit, die sofort in das aktuelle Risiko-Management und die IT-Security-Maßnahmen einbezogen werden können. Zudem liegen Auswertungen für das Management hinsichtlich der aktuellen Bedrohungslage vor, um weitere Entscheidungen zu treffen und Planungen durchführen zu können. Eine geeignetes Attack Surface Management läuft vollautomatisch und fortlaufend ab, so dass ein Unternehmen schnell Maßnahmen ergreifen kann und auch zukünftig immer auf dem aktuellen Stand ist. So verlieren Cyberkriminelle schnell die Lust, ihre Spurensuche fortzusetzen, da sie keine Angriffsflächen finden. Man entzieht ihnen so ihre Basis und verhindert ein kriminelles Vorgehen in den eventuell auffindbaren und verwundbaren Systemen auf Kosten des Unternehmens.

Stijn Vande Casteele,
Founder & CEO
bei Sweepatic