ANLEITUNG FÜR DAS SCHWACHSTELLEN-MANAGEMENT

Whitepaper von F-Secure

F-Secure

INHALT

MANAGEMENTÜBERSICHT

Umfassendes Bedrohungsmanagement

F-Secure Radar ist eine komplette, einfach zu implementierende All-in-one-Plattform für Schwachstellen-Scanning und -Management, die die Sicherheitsprogramme von Unternehmen mit klaren, umsetzbaren und priorisierten Erkenntnissen über reale Risiken unterstützt. Radar als Lösung mit einem effizienten Schwachstellen-Management wurde speziell für kleine und mittlere Unternehmen (KMU) konzipiert, um deren geschäftliche Kontinuität zu gewährleisten. Nicht gepatchte sowie unzureichend konfigurierte Software bietet ideale Angriffsflächen und Sicherheitslücken für Hacker. Mit F-Secure Radar lassen sich die Kosten für Cybersicherheit deutlich senken, und zwar durch die Erkennung potenzieller Sicherheitsprobleme, bevor diese für Angriffe ausgenutzt werden können. Aufgrund der Cloud-Ressourcen ist Radar eine kostengünstige Lösung. Das spielt besonders für Kleinunternehmen eine wichtige Rolle, die über keine speziellen Sicherheitsmaßnahmen verfügen.

Darüber hinaus gilt F-Secure Radar als optimale Lösung für Managed Service Provider (MSP), die damit den Umsatz steigern und das Marktpotenzial ausschöpfen können. Radar versetzt MSP in die Lage, ihr Serviceangebot um cloudbasiertes Schwachstellen-Management zu erweitern. Dadurch können diese Firmen skalierbare und kostengünstige Cyber-Security-Lösungen auf Marktführerniveau anbieten.

Endkunden, die weder die Zeit noch das Know-how für eigene Schwachstellenanalysen haben, setzen ihre Cybersicherheitsstrategien höchstwahrscheinlich mithilfe lokaler Servicepartner um. Die Datenschutz-Grundverordnung (DSGVO) der EU hält Kundenunternehmen dazu an, die Einhaltung aktueller Richtlinien zu verbessern und sich dabei von solchen Anbietern beraten und unterstützen zu lassen. Diese Firmen bedienen zumeist Endkunden mit maximal tausend Arbeitsplätzen.

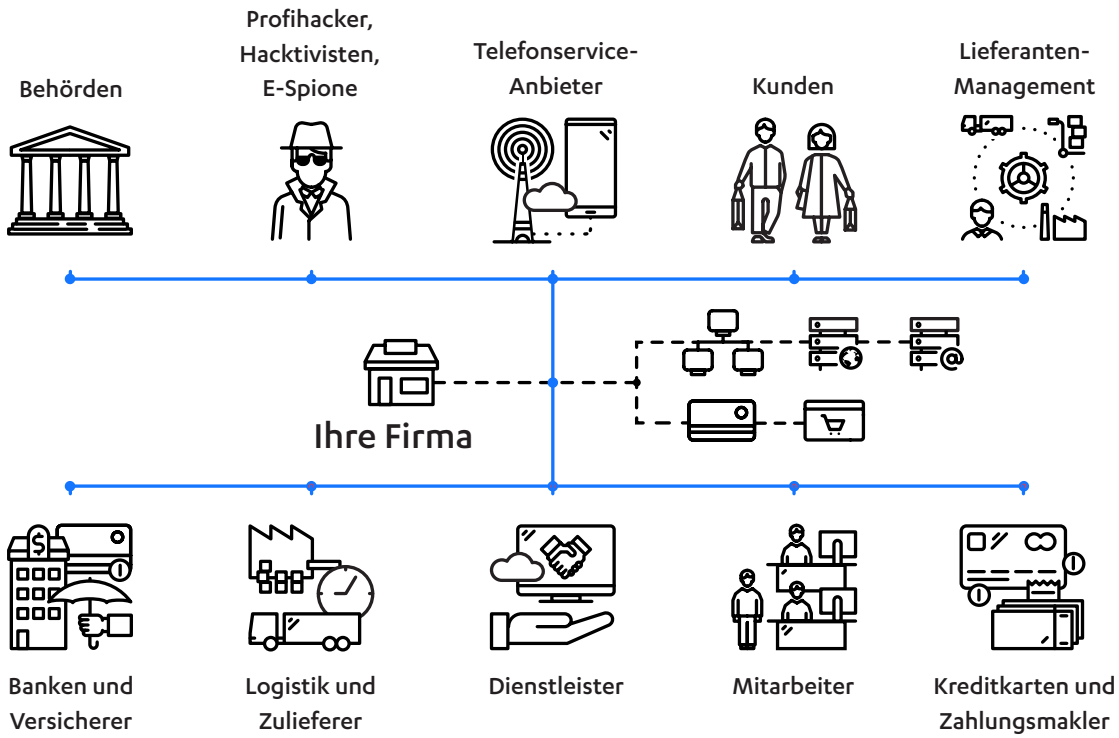
Dieses Dokument beschreibt die Hochsicherheitskontrollen von F-Secure Radar.

Identifizierung und Offenlegung möglicher Bedrohungen

Im Gegensatz zu vielen anderen Lösungen für Schwachstellen-Management setzt F-Secure Radar eine Web-Crawling-Technologie ein, die auch als „Internet Asset Discovery" bezeichnet wird. Diese deckt sogar das Deep Web ab. Mit ihrer Hilfe lassen sich zahlreiche Aufgaben ausführen – von der Bedrohungsanalyse bis hin zur Business Intelligence. Mit Radar können Sie alle Ziele einfach und schnell auf Risiken und potenziell anfällige Verbindungen untersuchen und die Analyse Ihrer Angriffsfläche über das eigene Netzwerk hinaus erweitern.

Erfolgreiche Marken werden mit ihrem geistigen Eigentum oft zum Ziel betrügerischer oder böswilliger Attacken. Dazu gehören Markenschutzverletzungen, bei denen sich Dritte als Ihr Unternehmen ausgeben und Phishing-Seiten zur Täuschung oder Infizierung von Besuchern installieren. Beim Typosquatting sichern sich Dritte Domains, die Ihrer Marke im Wortlaut ähneln, um Datenverkehr mithilfe von Links umzuleiten. Viele Firmen sind sich solcher Aktivitäten kaum oder gar nicht bewusst.

DIE ZAHLREICHEN CYBERRISIKEN FÜR UNTERNEHMEN



Der Payment-Card-Industry-Data-Security-Standard (PCI-DSS)

Erfüllung aktueller und zukünftiger gesetzlicher Richtlinien

Als zugelassener Dienstleister ist F-Secure verpflichtet, die hier aufgelisteten Aktionen durchzuführen, um etwaige Abweichungen der vom Scankunden bereitgestellten Informationen zu ermitteln. Infos zu solchen Unstimmigkeiten sind in der Scan-Konformitätsbescheinigung unter „Scan-Status" anzugeben. Diese Daten müssen zwar wie beschrieben gemeldet werden, trotzdem müssen wir sie dann zwecks Prüfung der PCI-DSS-Compliance außer Acht lassen:

- Einbeziehung aller IP-Adressen oder Domänen, die F-Secure bereits zur Verfügung gestellt wurden. Auch Adressen oder Domains, die sich immer noch im Besitz des Scankunden* befinden oder von ihm verwendet und auf seinen Wunsch entfernt wurden, finden Beachtung.
- Falls der Scankunde eine IP-Adresse oder Domain nicht mehr besitzt oder verwaltet: Einbeziehung dieser IP-Adresse oder Domain für mindestens ein weiteres Quartal, nachdem sie aus dem Gültigkeitsbereich entfernt oder vom Scankunden freigegeben wurde.
- Überprüfung der IP-Adresse jeder angegebenen Domain, um festzustellen, ob sie bereits vom Scankunden zur Verfügung gestellt worden ist.
- Durchführung einer DNS-Vorwärts- und -Rückwärtssuche für jede angegebene Domain nach allgemeinen Hostnamen (zum Beispiel „www" oder „mail"), die nicht vom Scankunden bereitgestellt wurden.
- Identifizierung aller IP-Adressen, die im Rahmen der DNS-Suche für MX-Einträge gefunden wurden.
- Identifizierung aller IP-Adressen außerhalb des Zielbereichs, die über Webumleitungen von In-Scope-Webservern erreicht werden können (deckt alle Formen der Umleitung ab, einschließlich JavaScript, Meta Redirect und HTTP 30x Codes).
- Abgleich von beim Crawling gefundenen und vom Benutzer bereitgestellten Domänen, um undokumentierte Domains des Scankunden zu identifizieren.

F-SECURE RADAR IM ÜBERBLICK

Alles im Blick

Abbildung aller Systemressourcen für einen Überblick über die Sicherheitslage. Kein System ist zu groß, F-Secure Radar lässt sich flexibel mit dem Firmenwachstum skalieren.

Kontinuierliche Verbesserungen

F-Secure Radar wird automatisch aktualisiert, optimiert und lässt sich über die F-Secure-Radar-API in Drittsysteme integrieren.

Effizientes Sicherheitsmanagement

Schwachstellenüberwachung mit automatischen Scans. Zuweisung, Verwaltung und Überwachung aller Sicherheitsprobleme in Abstimmung mit Systemadministratoren, Entwicklern oder Prüfern.

Konformität mit EU-Richtlinien

F-Secure Radar erfüllt die EU-Vorschriften mit der PCI-ASV-Konformität zum Scannen von Sicherheitslücken und hilft Kunden bei der Einhaltung der DSGVO.

Einfache benutzerdefinierte Berichterstattung

Passen Sie standardisierte Berichte für alle Zielgruppen in verschiedenen Formaten an und automatisieren Sie sie.

F-Secure Radar individuell für Sie

Führen Sie Schwachstellen-Scans über eine sichere, cloudbasierte Software-as-a-Service-Lösung (SaaS) oder als lokale Option hinter der Firewall Ihres Unternehems durch.

DIE GESCHICHTE VON EQUIFAX

Am 7. September 2017 gab der Kreditbewerter Equifax bekannt, dass er Opfer eines Cyberangriffs geworden war, bei dem auf personenbezogene Daten von bis zu 145,5 Millionen Menschen zugegriffen wurde. Dieser Vorfall führte zur vorzeitigen Pensionierung des damaligen Hauptgeschäftsführers sowie von zwei hochrangigen Sicherheitsbeauftragten des Unternehmens.

Eine forensische Analyse ergab, dass die Angreifer eine nicht gepatchte Schwachstelle in der Webanwendungssoftware Apache Struts von Equifax ausgenutzt hatten. Für die Sicherheitslücke, die ursprünglich vom chinesischen Sicherheitsforscher Nike Zheng entdeckt worden war, hatte Apache am 6. März 2017 ein Update veröffentlicht. Am 9. März 2017 wurde die Schwachstelle bereits aktiv ausgenutzt.

Equifax wurde – wie alle anderen Firmen, die die Plattform nutzen – am 6. Mai 2017 auf den Patch aufmerksam gemacht. Eine entsprechende Nachricht erhielten am 9. Mai 2017 alle IT-Mitarbeiter. Allerdings führten interne Missverständnisse sowie eine Reihe erfolgloser Untersuchungen dazu, dass Equifax die gefährdeten Apache-Installationen erst ab 29. Juli 2017 umfassend patchte, als aus Sicht des Unternehmens Nachweise für eine Sicherheitsverletzung vorlagen.

Wie sich herausstellte, hatten sich Angreifer am 13. Mai 2017 Zugang zu den Systemen von Equifax verschafft, also genau eine Woche nach der Veröffentlichung des Patches. Eine genauere Untersuchung ergab, dass Equifax eine 48-Stunden-Richtlinie für die Anwendung kritischer Patches implementiert hatte, diese aber nicht eingehalten wurde. Sonst hätte die Firma die Sicherheitsverletzung erfolgreich abwehren können.

Equifax brauchte fast drei Monate, um die kritische Schwachstelle zu patchen. Eine lange Zeit, aber es existieren zahlreiche Unternehmen, die noch viel langsamer reagieren. So gibt es selbst heute noch viele aktive Systeme, die für EternalBlue Exploits anfällig sind, die im Sommer 2017 zu den Angriffen durch die Trojaner NotPetya und WannaCry geführt hatten. Die Geschichte von Equifax mag etwas chaotisch klingen. Für Teams, die mit der Verwaltung komplexer Computerinfrastrukturen beschäftigt sind, gleicht das aber eher dem Normalzustand.

Patching ist keine Selbstverständlichkeit

Patching zählt nicht zu den Selbstverständlichkeiten. Die Installation von Software-Updates in einer Firma ist häufig die Aufgabe mehrerer Personen. Mechanismen zur Anwendung von Updates sowie Benachrichtigungen zu verfügbaren Patches unterscheiden sich teilweise so deutlich wie Betriebssysteme oder Software untereinander. Jeder Anbieter hat seine eigene Methode, seine Kunden über die Verfügbarkeit von Updates zu informieren. Und da es auch keinen zentralen Ort gibt, über den man alle Informationen abrufen kann, halten sich IT-Abteilungen immer noch gern per E-Mail und RSS-Feeds auf dem Laufenden.

Da IT-Abteilungen Dutzende oder Hunderte Einzelanwendungen verwalten müssen, für die regelmäßig Updates und Patches ausgegeben werden, kann man sich das Chaos ungefähr vorstellen. Zumindest eine Person muss verstehen, welche Änderungen die Software erfahren hat und wie sich diese auf die einzelnen Systeme auswirken. Deshalb müssen Updates vor der Implementierung oft in der gesamten Firma in Form von Pilotprojekten getestet werden. Bei Servern ist dazu die Planung von Wartungsfenstern notwendig, wenn es durch das Patching zu Ausfallzeiten kommt. Dadurch sind IT-Abteilungen dazu gezwungen, Updates zu priorisieren und Patches im Allgemeinen nur dann zu installieren, wenn dies unbedingt nötig ist.

Um aber wiederum effektive Entscheidungen zur Priorisierung treffen zu können, müssen sie wissen, ob eine Schwachstelle aktiv ausgenutzt wird beziehungsweise Bestandteil der Angriffsfläche des Unternehmens ist.

Bekannte Unbekannte und unbekannte Unbekannte

Um die Computerinfrastruktur ordnungsgemäß abzusichern, muss das IT-Personal wissen, welche Systeme gepatcht gehören. Dafür müssen zumeist alle bekannten Systeme und Softwareprogramme einer Organisation inventartechnisch erfasst und gepflegt werden. Wenn Firmen wachsen, implementieren manche Geschäftsspartner gern ihre eigenen Systeme und Anwendungen, und zwar ohne Beteiligung der IT-Abteilung. Diese Systeme fassen wir unter dem Oberbegriff Schatten-IT zusammen – sie können die Angriffsfläche eines Unternehmens erheblich vergrößern. Sie sind nur schwer aufzuspüren, hinzu kommt noch, dass ihre Auswirkungen häufig stark unterschätzt werden.

Aber wenn Schatten-IT-Systeme schon zu den bekannten Unbekannten zählen, dann verbirgt sich hinter den Systemen der Lieferkette eines Unternehmens eine noch größere Gefahr: eine quantitativ höhere Anzahl an unbekannten Unbekannten. Und Angriffe auf die Lieferkette geschehen ziemlich häufig.

Während der Weihnachtszeit 2013 verschafften sich Kriminelle die Kreditkartendaten von mehr als 60 Millionen Kunden der großen US-Einzelhandelskette Target. Sie konnten in das Netzwerk von Target eindringen, indem sie Malware über einen E-Mail-Anhang auf einem System installierten, das einem Unternehmen namens Fazio Mechanical gehörte. Damals stellte Fazio Mechanical Heizungs- und Klimaservices für Target bereit. Durch die Attacke sicherten sich die Angreifer die VPN-Anmeldeinformationen für die Remote-Verbindung mit dem Unternehmensnetzwerk von Target, über das sie wiederum auf den Registrierkassen in geschätzten 1.800 Filialen des Unternehmens Schadsoftware installierten. Untersuchungen des Vorfalls ergaben, dass es keinerlei Zugangskontrollen zu den Systemen gab, dazu zählten auch Ladengeräte wie POS-Kassensysteme und -Server. In einem Fall konnten die Verbrecher sogar direkt mit den Registrierkassen kommunizieren, nachdem sie sich über eine Fleischwaage der Feinkostabteilung eines anderen Geschäfts eingeschleust hatten.

Angriffsziel Intranet

Während das Patching von Schwachstellen in Strukturen mit Internetanschluss im Allgemeinen ernst genommen wird, wird die Sicherheit von Systemen hinter der Firmen-Firewall häufig vernachlässigt. Viele Mitarbeiter nehmen an, dass sie gegen Eindringlinge geschützt sind. Diese Sicherheitsmängel hängen jedoch nicht immer mit den Software-Patch-Levels zusammen. Nicht selten sind es Fehlkonfigurationen, die Angreifern den Zugriff auf einfache Lateral-Movement-Mechanismen und somit das unauffällige Auskundschaften von Daten nach dem ersten Zugriff ermöglichen.

Die Identifizierung von Software-Fehlkonfigurationen kostet viel Zeit und Mühe. Hinzu kommt, dass Software nicht immer sofort nach der Installation sicher arbeitet. Häufig müssen Nachforschungen angestellt werden, um herauszufinden, wie die einzelnen Bestandteile der IT-Infrastruktur eines Unternehmens ordnungsgemäß konfiguriert gehören. Nehmen Sie zum Beispiel einen SSH-Server: Nach der Installation möchten Sie ihn wahrscheinlich so konfigurieren, dass keine Passwortanmeldungen zulässig sind beziehungsweise die Funktion für den Remote-Log-in als Root-Benutzer deaktivieren. Ein neuer Administrator, der ein System einrichtet, muss wissen, dass und wie diese beiden Konfigurationsänderungen vorgenommen werden. Nehmen wir an, es befinden sich einige SSH-Server in Ihrem Netzwerk, die alle zu unterschiedlichen Zeiten von unterschiedlichen

Mitarbeitern installiert worden sind. Um zu ermitteln, ob ein Server falsch konfiguriert ist, müssen Sie alle prüfen. Stellen Sie sich nun vor, dass Sie das gleiche Prinzip auf die zahlreichen in einem Unternehmen installierten Softwarekomponenten sowie auf Einstellungen der Betriebssysteme selbst anwenden müssen. Schon die einmalige Ausführung dieser Aufgabe gestaltet sich komplex –ganz zu schweigen davon, wenn sie mehrmals durchgeführt werden muss. Aus diesem Grund haben Aufgaben wie diese Priorität.

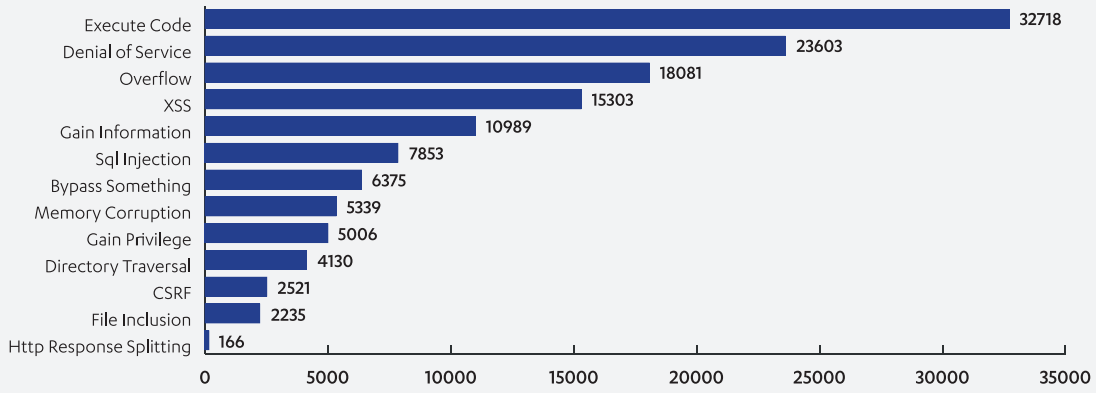
Transparenz als Schlüssel

Die Sicherheit von Systemen gestaltet sich äußerst komplex und arbeitsintensiv. Letztlich erweist es sich jedoch als wichtig, sich ein klares und präzises Bild von Ihrer aktuellen Situation zu machen. Erst dann können Sie sich der Aufgabe der ordnungsgemäßen Sicherung Ihrer Infrastruktur widmen. Bis dahin sollten Sie in der Lage sein, folgende Fragen zu beantworten:

- Ist unsere Risikostufe annehmbar?
- Wie hoch ist die Wahrscheinlichkeit für eine Sicherheitsverletzung?
- Was wären die wahrscheinlichen Auswirkungen dieser Blessur?
- Welche unserer Güter und Werte sind am stärksten gefährdet?
- Wie können wir das Risiko für unsere Güter und Werte in Zukunft reduzieren?
- Wie viel müssen wir investieren, um eine für uns akzeptable Risikostufe zu erreichen?
- Wie passen diese Kosten in die aktuellen Budgetvorgaben?

Diese Fragen sollte sich jedes Führungsteam der IT-Abteilung stellen, wenn es wirklich um die Cybersicherheit besorgt ist (was selbstverständlich so sein sollte). Mit einer entsprechenden Transparenz der Infrastruktur Ihrer Firma (einschließlich der bekannten Unbekannten und unbekannten Unbekannten) können Sie diese Fragen nicht nur vorausschauend und sicher beantworten, sondern auch nachts besser schlafen.

ÜBERSICHT: AKTUELLE SCHWACHSTELLEN



Quelle: http://www.cvedetails.com/vulnerabilities-by-types.php

Proaktive Vermeidung von Vorfällen

Da die Zahl der Cyberbedrohungen ständig steigt, müssen CIOs dem Thema Sicherheit höchste Priorität einräumen. Cyberkriminalität gilt heute als Milliarden-Dollar-Geschäft – Tendenz steigend. Nach Angaben von Arbor Networks stiegen Anzahl und Größe von Cyberangriffen im Jahre 2017 um 73 %. Angesichts dieser stetig wachsenden Gefahr kann sich kein Unternehmen, egal ob klein oder groß und unabhängig von der Branche, vor dem Risiko einer Datenverletzung sicher fühlen. Es geht nicht mehr darum, ob Ihre Firma angegriffen wird, sondern wann. Aus diesem Grund ist es wichtiger denn je, einen proaktiven Sicherheitsansatz zu verfolgen.

Weil zahlreiche Firmen irrtümlich davon ausgehen, dass die Implementierung von Sicherheitsmaßnahmen einen hohen Zeit- und Kostenaufwand erfordert, beschränken sich viele auf eine eher abwartende Strategie. Man wartet, bis man selbst betroffen ist – und verankert erst dann eine Lösung. Allerdings wird diese Methode Ihre Firma am Ende wahrscheinlich viel teurer zu stehen kommen als die Ergreifung von Präventivmaßnahmen. Statistiken zeigen, dass sich die Investition in solche Maßnahmen im Falle eines Angriffs ganz schnell amortisiert.

Der Schlüssel zur Verhinderung von Cyberattacken

Um Sicherheitsverletzungen durch menschliches Versagen zu reduzieren, muss man ein Umfeld schaffen, in dem alle Mitarbeiter ein Interesse an Sicherheit haben. Das heißt, Ihre Angestellten müssen den Wert des Schutzes von Kunden- und Partnerinformationen sowie ihre Rolle dabei verstehen. Dazu benötigen sie Grundkenntnisse in puncto Risikolandschaft sowie eine Strategie für vernünftige Entscheidungen in Bezug auf die Internetsicherheit. Viele Menschen verstehen unter Sicherheit einen gesunden Menschenverstand, in Wahrheit aber herrscht eher der Grundsatz „Aus den Augen, aus dem Sinn“. Die Schaffung einer Basis für Sicherheit muss mit der Aus- und Fortbildung der Belegschaft beginnen.

Technologie-Fortschritte führen zu aufregenden Sicherheitslösungen. Allerdings entwickeln auch Angreifer ständig neue Taktiken und Techniken, um diese zu überwinden. Sicherheit muss nicht teuer sein, das Nichtstun scheidet als Option aus. Unabhängig davon, ob sich ein Unternehmen eine neue Hightech-Sicherheitslösung leisten kann oder nicht, sollte immer Zeit sein, ein durchdachtes Sicherheitskonzept zu entwickeln. Proaktives Verhalten zählt zum Pflichtprogramm und erfordert Wachsamkeit. Durch Standardprozesse, -verfahren und -richtlinien für die Sicherheit und Mitarbeiterschulung reduzieren Firmen ihre Anfälligkeit für Attacken deutlich.

IHRE ACHILLESFERSE: EINE EINZIGE SCHWACHSTELLE REICHT AUS

Alle

90 **Minuten**

wird mindestens eine neue Sicherheitsschwachstelle identifiziert

Das macht durchschnittlich

7 **Schwachstellen**

pro Asset in einer typischen IT-Umgebung

Das macht durchschnittlich

8.000

bekannte und unbekannte Schwachstellen pro Jahr

50-300

kritische Schwachstellen

bieten Angriffsflächen (je nach Branche)

Es benötigt im Schnitt

103 **Tage,**

bis bekannte Sicherheitsdefizite behoben werden

Es dauert im Durchschnitt

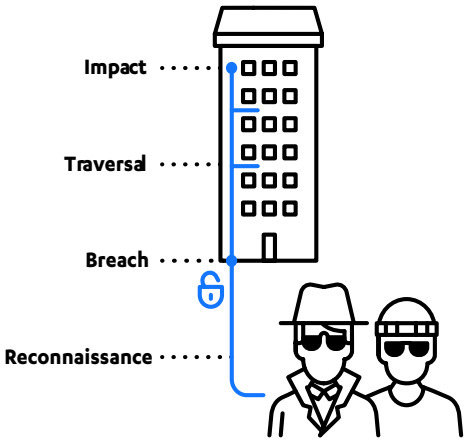
15 **Tage,**

bis eine Schwachstelle ausgenutzt wird

DIE TYPISCHE CHRONOLOGIE EINES ANGRIFFS

Im Fachjargon für Computersicherheit steht „Day Zero" für den Tag, an dem die betroffene Partei (vermutlich der Anbieter des attackierten Systems) von einem Angriffspunkt erfährt. Bis zu diesem Tag wird sie als „Zero-Day-Schwachstelle" bezeichnet. In ähnlicher Weise würde man eine Sicherheitslücke, die seit 30 Tagen bekannt ist, eine „30-Tage-Schwachstelle" nennen. Sobald der Anbieter von einer Schwachstelle erfährt, erstellt er üblicherweise einen Patch oder schlägt Problemlösungen vor.

Im Allgemeinen wird um Zero-Day-Schwachstellen zu viel Wind gemacht. Die Schwachstellen-Datenbank CVE Details zeigt im Schnitt einen Risikowert von 6,8 für alle bekannten Schwachstellen auf allen bekannten Plattformen. Von den dort über 80.000 registrierten Schwachstellen sind 12.000 (fast 15 %) mit einem hohen Schweregrad klassifiziert. Man sollte dabei aber bedenken, dass Schwachstellen in vielen verschiedenen Client- und serverseitigen Anwendungen (einschließlich Adobe Flash) existieren.



Aus Firmensicht muss der Umgang mit schweren Schwachstellen oberste Priorität genießen. Gut geführte Organisationen sind in der Lage, dies erfolgreich zu praktizieren. Schwachstellen mit hohem Schweregrad werden deshalb auch umgehend gepatcht. Natürlich besteht nicht die gesamte Angriffsfläche Ihres Unternehmens aus solchen Sicherheitslücken. Ihr Chief Information Security Officer sorgt sich wahrscheinlich mehr um Phishing- und Upstream-Attacken als um interne Fehlkonfigurationen des Netzwerks oder nicht gepatchte interne Systeme. Als IT-Administrator lautet Ihr oberstes Gebot: Pflege der Infrastruktur.

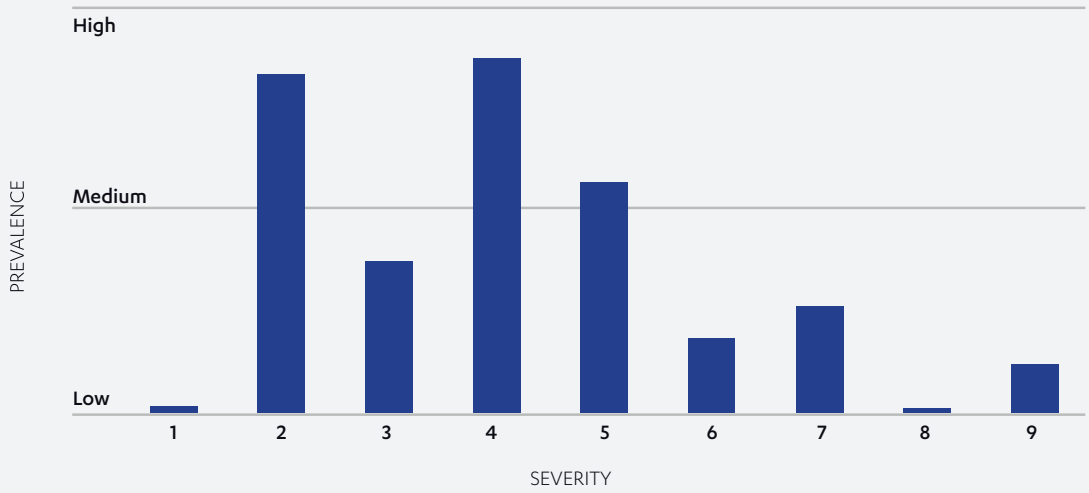
So führen Sie sicher sofort eine Sichtung des Systems durch, wenn ein schwerer Angriffspunkt ans Licht kommt. Aber was ist mit dem Rest? Patches können nicht sofort nach ihrer Veröffentlichung auf jede Software in jedem System Ihres Netzwerks angewendet werden. Aus diesem Grund beheben IT-Administratoren Schwachstellen mit geringem Schweregrad – wenn überhaupt – im Rahmen regelmäßiger Patch-Zyklen. Die meisten von ihnen verfügen einfach nicht über die Zeit, die Auswirkungen jeder neuen Sicherheitslücke genau zu untersuchen.

Deshalb ignorieren sie sie häufig. Bei der Anwendung von Patches stellen Administratoren oft Fragen wie:

- Wie exponiert ist das System?
- Wird dieser Patch andere Komponenten oder Systeme negativ beeinträchtigen?
- Habe ich überhaupt Infos zu dieser Schwachstelle und ihrem Bedrohungspotenzial?

Die bei unseren Stammkunden mit unserem RADAR-Service durchgeführten Analysen von Trends hat Folgendes gezeigt: Sicherheitslücken mit hohem Schweregrad waren selten bis gar nicht anzutreffen. Die überwiegende Mehrheit der identifizierten, nicht gepatchten Sicherheitslücken besaß einen geringen bis mittleren Schweregrad. Ein interessantes Detail dabei war, dass TLS/SSL- und OpenSSH-Fehlkonfigurationen ziemlich oft auftraten. Beachten Sie jedoch, dass die Systeme möglicherweise auf diese Weise angepasst wurden, um eine gute Interoperabilität mit Kunden, Partnern oder proprietären internen Diensten zu gewährleisten.

Unser Information Security Manager hat sich diese Grafik angesehen und kam zu dem Schluss, dass er ruhig schlafen könnte, wenn die Ergebnisse die Lage in unserem eigenen Unternehmen widerspiegeln würden.



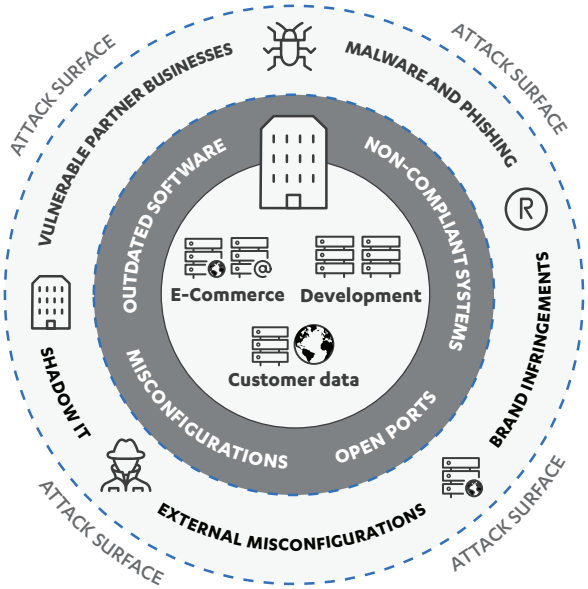
Die Daten in dieser Grafik entstammen einer Studie des Kundenstamms von F-Secure aus dem ersten Halbjahr 2018 mit unserem Radar-Produkt. F-Secure Radar ist eine Schwachstellen-Management- und Sicherheitsscanning-Lösung, mit der Plattformen und Webanwendungen auf Sicherheitslücken überprüft werden.

DIE FOLGEN EINER UNZUREICHENDEN ÜBERWACHUNG IHRER ANGRIFFSFLÄCHE

Die Risiken

Die Einrichtung und aktive Pflege einer sicheren Konfiguration für ICT-Systeme gilt als wichtigste Sicherheitskontrolle. ICT-Systeme, die nicht geschützt, verstärkt oder gepatcht werden, sind besonders anfällig für Angriffe, die normalerweise leicht verhindert werden könnten.

Unternehmen, die keine eigenen Sicherheitsrichtlinien für eine sichere Konfiguration sowie das Patching ihrer ICT-Systeme erstellen und implementieren, setzen sich folgenden Risiken aus:



Unbefugte Systemänderungen

Angreifer können unerlaubte Änderungen an ICT-Systemen oder -Informationen vornehmen, die die Vertraulichkeit, Verfügbarkeit und Integrität von Strukturen gefährden.

Ausnutzung ungepatchter Schwachstellen

Fast täglich werden neue Patches veröffentlicht, deren zeitnahe Anwendung für die Gewährleistung der Sicherheit von ICT-Systemen eine unerlässliche Rolle spielt. Hacker versuchen, sich über ungepatchte Punkte unbefugten Zugriff auf Systemressourcen und Informationen zu verschaffen. Viele erfolgreiche Attacken werden durch das Ausnutzen einer Schwachstelle ermöglicht, für die bereits ein Patch vorlag.

Ausnutzung unsicherer Systemkonfigurationen

Angreifer können ungeschützte oder kaum gesicherte Systeme ausnutzen und dadurch ...

- ... unbefugten Zugriff auf Informationsressourcen erlangen oder Malware einschleusen.
- ... nicht mehr länger benötigte, aber nicht entfernte oder deaktivierte Funktionen nutzen, um Attacken durchzuführen und unbefugten Zugriff auf Systeme, Dienste, Ressourcen und Informationen zu erlangen.
- ... nicht autorisierte Geräte verbinden, um Informationen zu infiltrieren oder Malware zu installieren.
- ... eine Hintertür für zukünftige Angriffe einrichten.

Anstieg der Sicherheitszwischenfälle

Ohne entsprechendes Know-how zu Schwachstellen sowie der Verfügbarkeit (oder Nichtverfügbarkeit) von Patches und Fixes können Sicherheitsvorfälle zunehmend zu Geschäftsausfällen führen.

Sicherheitsverletzungen schaden Kleinunternehmen am stärksten

Lediglich 31 % aller Kleinunternehmen ergreifen aktive Maßnahmen, um sich zu schützen. Darüber hinaus sind sich 41 % von ihnen nicht über die mit menschlichem Versagen verbundenen Risiken im Klaren, und nur 22 % erklären sich bereit, ihre Sicherheitsvorkehrungen gegenüber dem Vorjahr zu verstärken.

Es überrascht vielleicht nicht, dass Sicherheitslücken bei Kleinunternehmen den größten Schaden verursachen. Mehr als 70 % aller Angriffe richten sich gegen solche Firmen. Schätzungen zufolge stehen 60 % aller attackierten KMU nach sechs Monaten vor der Geschäftsaufgabe. Die Studienergebnisse sind möglicherweise leicht verzerrt, weil die Zahl derjenigen, die das Thema Cybersicherheit ignorieren, hoch ist. Viele Firmen halten traditionelle Sicherheitsmaßnahmen wie Antivirus-Programme und Firewalls noch für mehr als ausreichend.

Die Wiederherstellungskosten von Datenschutzverletzungen sind höher, als man denkt

Ein Mangel an Informationen und die Gefährdung durch Bedrohungen haben zu einem drastischen Anstieg der Angriffe geführt: Der Anteil der Datenschutzverletzungen durch Cyberattacken ist von 18 % im Jahr 2014 auf mittlerweile 31 % angewachsen. Wenn Sie glauben, dass Sie bei einem Angriff mit dem Schrecken davonkommen, liegen Sie falsch: Die Wiederherstellungskosten sind enorm hoch und führen nicht selten zu Firmenschließungen. Die Durchschnittskosten für die Wiederherstellung nach Datenschutzverletzungen bei KMU betragen 36.000 US-Dollar und können auf bis zu 50.000 Dollar steigen. Dieser Betrag kann den Gesamtwert eines Kleinunternehmens ausmachen. Für die Opfer kann eine Wiederherstellung nahezu unmöglich sein.

Da sich die meisten kleinen Firmen nicht von solchen Sicherheitsvorfällen erholen, sind sie gut beraten, Vorsichtsmaßnahmen zu ergreifen.

Die firmeninterne Diskussion zum Thema Cyberrisiken

Wendet sich ein CISO mit einer Budgetanfrage für eine neue Technologie oder Sicherheitsinitiative an die Geschäftsführung, kommt es zu einem Treffen zwischen Personen, die nicht die gleiche Sprache sprechen. CFO und CEO denken in Geldbeträgen – Geschäftswert und ROI. Kann der CISO nicht mit solchen Fakten argumentieren, muss er das Topmanagement anders von der Investition überzeugen. Er greift auf das Argument zurück, auf das Führungskräfte reagieren: Angst. „Wenn wir das nicht tun, bricht irgendwann alles zusammen."

Schließlich möchte kein Unternehmen aus den falschen Gründen für Schlagzeilen sorgen.

Aber woher weiß man, ob durch solche Investitionen in die Sicherheit Risiken effektiv reduziert oder eliminiert werden, wie sich das die Führungsetage erhofft? Was bringen die teure Mitarbeiterweiterbildung, das Ereignisüberwachungssystem und der Austausch von Sicherheitssoftware im Unternehmen? Wie kann eine Firma sicher sein, dass sie an den richtigen Stellen investiert? Ob sie die geeignete Versicherung abgeschlossen hat, um sich im Falle von Datenverletzungen, Ransomware-Vorfällen oder DDoS-Angriffen zu schützen?

Und wie weist der CISO dem Topmanagement nach, dass diese Ausgaben für die Organisation enorm wichtig sind, ohne bei seiner Argumentation auf das FUD-Prinzip (Fear, Uncertainty, Doubt – Furcht, Ungewissheit und Zweifel) zurückzugreifen?

Die Antwort lautet: Er muss in der Lage sein, die Auswirkungen von Cyberverletzungen für das Unternehmen quantifizieren zu können – etwas, vor dem die meisten CISOs zurückschrecken. Es stimmt, dass der Einsatz mehrdeutiger Bewertungssysteme oder einer roten, grünen und gelben Farbcodierung zur Angabe von Risiken nicht gerade sehr aussagekräftig ist.

„Die meisten Manager stützen sich auf qualitative Leitlinien aus sogenannten ‚Heatmaps', die ihre Verwundbarkeit als ‚niedrig' oder ‚hoch' beschreiben, ein Konzept, das wiederum auf vagen Schätzungen basiert, die häufige kleine und seltene große Verluste zusammenfassen", schreiben Chacko, Sekeris und Herbolzheimer in ihrem „Harvard Business Review"-Artikel „Can you put a Dollar amount on your companys cyber risk" vom 5. Oktober 2016. „Dieser Ansatz hilft Managern jedoch nicht zu verstehen, ob sie ein 10- oder 100-Millionen-Dollar-Problem haben, geschweige denn, ob sie in Malware-Verteidigungsprogramme oder E-Mail-Schutz investieren sollten. Folglich treffen Unternehmen bei der Priorisierung ihrer Cybersicherheit-Funktionen weiterhin falsche Entscheidungen und wählen oft einen unzureichenden Versicherungsschutz."

Es funktioniert jedoch, Risikobewertungen für die Sicherheit mit realistischen Zahlen zu erstellen. Es ist möglich, in einer Sprache zu sprechen, die man auch im Konferenzraum der oberen Etage versteht.

„Die Implementierung dieser Technologie kostet 100.000 US-Dollar, reduziert jedoch unser Risiko um zwei Millionen US-Dollar." Oder: „Wir können unseren Cyberversicherungsschutz um 50 Millionen US-Dollar reduzieren. Und hier ist der Grund dafür." Dies sind Aussagen, die CISOs und CFOs mithilfe neuer Methoden zur Messung und Quantifizierung von Cyber-Security-Risiken guten Gewissens tätigen und nachweisen können. Die Methode von F-Secure heißt „Cyber Breach Impact Quantification" (CBIQ) und prognostiziert, wie viel ein Cybervorfall eine Firma vermutlich kosten wird. Sie demonstriert außerdem, um welchen Prozentsatz Unternehmen ihr Risiko durch die Implementierung einer spezifischen Sicherheitskontrolle reduzieren können.

Allgemeiner Überblick: 2019 Cost of Data Breach Study

IBM Security und Ponemon Institute, Ergebnisse der von Juli 2018 bis April 2019 durchgeführten Studie:

- Weltweit untersuchte Unternehmen: 507
- Durchschnittliche Gesamtkosten für eine Datenverletzung: 3,92 Millionen US-Dollar
- Durchschnittliche Kosten pro verlorenem oder gestohlenem Datensatz: 150 US-Dollar
- Durchschnittlicher Umfang einer Datenverletzung: 25.575
- Durchschnittliche Zeit bis zur Identifizierung und Eindämmung einer Datenverletzung: 279 Tage
- Wahrscheinlichkeit des Eintritts einer Datenverletzung in den nächsten beiden Jahren: 29,6 %

DSGVO – ANDROHUNG DRAKONISCHER GELDSTRAFEN ODER NEUE MÖGLICHKEITEN FÜR DIE EIGENE ORGANISATION?

Als ob die Wiederherstellungskosten nach einer Datenschutzverletzung nicht schon genug sind, kann es passieren, dass Firmen aufgrund von Verstößen gegen die Datenschutz-Grundverordnung (DSGVO) der EU auch noch mit heftigen Bußgeldern bestraft werden. Diese Richtlinie trat im Mai 2018 mit dem Ziel in Kraft, den Datenschutz für EU-Bürger sicherzustellen. So können Unternehmen, die Datenschutzverletzungen erleiden, mit Geldstrafen von bis zu vier Prozent ihres Jahresumsatzes oder 20 Millionen Euro belegt werden – je nachdem, welcher Wert höher ist.

Auch wenn die DSGVO klar auf die EU abzielt, beschränkt sich ihr Geltungsbereich nicht zwingend auf Europa. So schreibt sie vor, dass sie von jedem Unternehmen eingehalten werden muss, das personenbezogene Daten von EU-Bürgern verarbeitet, speichert oder überträgt. Diese recht breite Definition betrifft so praktisch jede Organisation mit einem Webauftritt. Da die DSGVO wahrscheinlich als Vorlage für andere Länder dienen wird, empfiehlt es sich, die eigenen Richtlinien, Verfahren und Technologien auf sie auszurichten, und zwar unabhängig davon, ob die jeweilige Firma technisch gesehen betroffen ist oder nicht. Datenschutzgesetze weltweit werden voraussichtlich eher strenger als lockerer werden.

Betrachten wir den Equifax-Vorfall durch die DSGVO-Brille: Damals wurden nach Schätzungen die personenbezogenen Daten von mehr als 147,9 Millionen Menschen offengelegt. Wäre das Unternehmen der DSGVO und der obligatorischen 72-Stunden-Frist für die Meldung festgestellter Verletzungen unterworfen gewesen, wäre es kläglich an den Anforderungen gescheitert. Equifax hat den Vorfall am 29. Juli 2017 bemerkt und ihn erst mehr als einen Monat danach, am 7. September, öffentlich gemacht. Legt man die im Rahmen der DSGVO mögliche Höchststrafe und den Equifax-Jahresumsatz von über drei Milliarden US-Dollar zugrunde, hätte die Firma mit einem Bußgeld von weit über hundert Millionen belegt werden können.

In puncto Sicherheit enthält die DSGVO keine spezifischen Anforderungen für den Datenschutz. Da die Implementierung solider Praktiken für die Sicherheit von Daten und die Einhaltung von Richtlinien entscheidend ist, sollte über ein umfassendes Sicherheitsprogramm nachgedacht werden. Dieses sollte Funktionen wie Bedrohungsprognosen, Prävention sowie die Erkennung und Bekämpfung von Sicherheitsverletzungen beinhalten. Ein effizientes Schwachstellen-Management ist ein kritischer Bestandteil dieses Programms und der DSGVO Compliance, wie der Equifax-Fall zeigt.

Zu den weiteren wichtigen Aspekten der DSGVO zählt das Dateninventar, also zu wissen, welche Informationen wo und/oder in Kopie in Ihrer Unternehmensinfrastruktur gespeichert sind. Die Erfassung und Dokumentation von Rechnern, auf denen Daten lagern, gilt als erster Schritt in diesem Prozess. Die Erkennungsscan-Funktionen von F-Secure Radar können Sie bei der Suche nach Netzwerk-Assets und Schatten-IT unterstützen. Zum Beispiel könnte ein von der Marketingabteilung für die Kampagne des Vorjahres eingerichteter Server möglicherweise Kundeninformationen enthalten, die nicht der DSGVO entsprechen.

Unter dem Strich kann man die DSGVO aus zwei verschiedenen Perspektiven betrachten: Entweder als Androhung drakonischer Strafen, die durch Einhaltung der Mindestanforderungen für die Compliance vermieden werden können. Oder als Möglichkeit, die Ziele der Richtlinie zu respektieren und Ihr Unternehmen proaktiv dahin zu manövrieren, wo es in unserer zunehmend datenorientierten Welt sein sollte.

DIE FUNKTIONALITÄT VON RADAR

Die beste Strategie bei Cyberbedrohungen ist, sie vorherzusagen und abzubilden.
Keine andere Technologie eignet sich hierfür besser als das Schwachstellen-Management.

Zur Angriffsfläche eines Unternehmens zählen Netzwerkinfrastrukturen sowie Software-, IOT- und Webanwendungen, sowohl intern als auch im globalen Internet. Man muss alle möglichen Interaktionspunkte auf dem Schirm haben und analysieren. Sicherheitsmanager sollten in der Lage sein, die Schwachstellen aus verschiedenen Perspektiven zu betrachten und zu bewerten. Nur so können sie Risiken einschätzen, Sicherheitsdefizite minimieren und die Vorschriften einhalten.

Im Gegensatz zu vielen anderen Schwachstellen-Management-Lösungen beinhaltet F-Secure Radar die Web-Crawling-Technologie (auch Internet Asset Discovery genannt), die sogar das Deep Web abdeckt. So lassen sich alle Ziele einfach und schnell auf Risiken und anfällige Verbindungen untersuchen und die Analyse Ihrer Angriffsfläche über Ihr eigenes Netzwerk hinaus erweitern.

Mögliche Bedrohungen identifizieren und entlarven

Wertvolle Marken und deren geistiges Eigentum machen Firmen oft zur Zielscheibe betrügerischer oder böswilliger Aktivitäten. Mithilfe von F-Secure Radar und ein bisschen Erfahrung sollte jeder IT-Sicherheitsmanager einen Bedrohungsanalysebericht über entsprechende Aktivitäten erstellen können, darunter Markenverletzungen oder Phising-Sites.

F-Secure Radar identifiziert alle Schwachstellen Ihrer Organisation und listet sie präzise auf. So können Sie Ihre Angriffsfläche minimieren und gleichzeitig Risiken mindern. Das IT-Sicherheitsteam kann mit dem Produkt den Sicherheitsstatus der Firma durch die Einbeziehung folgender Parameter abbilden:

- Schwachstellen bekannter, unbekannter und potenzieller Art, die für das Geschäft von Bedeutung sind
- Steuerelemente für jegliche Software, Hardware und Firmware sowie über alle Netzwerke
- Schatten-IT, von außen falsch konfigurierte Systeme, Malware-Websites, mit Websites verknüpfte Hosts
- Sicherheitsentropie von Partnern und Auftragnehmern
- Markenverletzungen und Phishing

SECURITY CENTER DASHBOARD
Behalten Sie jederzeit den aktuellen Überblick über Schwachstellen und Vorfälle, erstellen Sie Standard- und benutzerdefinierte Berichte zu Risiken und Compliance und mehr.

INTERNET ASSET DISCOVERY
Zeigen Sie potenzielle Angriffsmethoden mithilfe einer Internetanalyse auf.

AUFDECKUNGSSCANS
Bilden Sie Ihre Angriffsfläche mithilfe von Netzwerk- und Portscanning ab.

SCHWACHSTELLENSCANS
Scannen Sie Systeme und Webanwendungen auf öffentlich bekannte Schwachstellen.

SCHWACHSTELLEN-MANAGEMENT
Verwalten Sie Schwachstellen zentral mit Sicherheitswarnmeldungen und Forensik.

PCI-DSS-COMPLIANCE
Gewährleisten Sie die Erfüllung aktueller und zukünftiger Gesetzesanforderungen, um das Risiko eines Datenverlusts zu verringern.

Internet Asset Discovery

Mit Radar können Sie die mit dem Internet verbundenen Systeme Ihrer Firma identifizieren. Die Internet-Discovery-Funktion verwendet Crawling und Portmapping, um Daten auf öffentlichen Systemen zu erfassen. Die Datensuche funktioniert nach Kriterien wie Standort, Top-Level-Domain, Pay-Level-Domain, Schlüsselwörter, Host-Namen und IP-Adresse.

Sie können die erkannten Hosts zu einer Scangruppe hinzufügen, um sie entweder passiv oder aktiv nach Sicherheitslücken zu durchsuchen. Passive Scans suchen nach Schwachstellen, ohne eine Verbindung zum Ziel-Host herzustellen. Beim aktiven Scannen wird ein regelmäßiger Systemcheck auf dem Host ausgeführt. Die Internet-Asset-Discovery-Funktion beinhaltet Folgendes:

- Aufzählung der Angriffsflächen
- BGP (IP zu AS)
- Öffentliche Quellen (RIPE, Public BGP, CERNET)
- IP- & Service-Daten
- Portscans & Banner
- Domain-Namen
- Reverse DNS, Zonenübertragung, Brute Force
- Whois-Informationen
- Verknüpfung aller oben stehenden Kriterien
- Geolokalisierung
- Öffentliche/private Datenbanken

Aufdeckungsscans

Der erste Schritt des Workflow-Prozesses für Schwachstellen-Management und Sicherheitsüberwachung geschieht mit Radar Discovery. Sie können damit Hosts und Netzwerkgeräte in Ihrer Infrastruktur identifizieren (innerhalb definierter Netzwerkbereiche).

Die Funktion verwendet ICMP-PING-, TCP-SYN-, UDP-Scan- und Fragment-Scantechniken, um alle in einem Netzwerk verfügbaren Hosts aufzulisten. Darüber hinaus werden die Dienste identifiziert, die jeder Host zur Verfügung stellt beziehungsweise welche Betriebssysteme sie ausführen.

Um einen Aufdeckungsscan in Ihrem Netzwerk durchzuführen, müssen Sie lediglich die erforderlichen Informationen in den IP-Bereich eingeben. Zu den weiteren Konfigurationsoptionen zählen:

- TCP-Portscanning und Definition des Portbereichs
- UDP-Portscanning und Definition des Portbereichs
- Begrenzung des Portbereichs auf die gängigsten hundert oder tausend offenen Ports
- Aktivierung der Diensterkennung für die erkannten Hosts
- Identifizierung des Betriebssystems auf jedem Live Host
- Scannen von Hosts, die nicht auf PING-Anfragen reagieren
- Kontrolle der Scanleistung durch die Konfiguration einer zusätzlichen Zeitverzögerung zwischen aufeinanderfolgenden Paketsätzen
- Steuerung der Anzahl der gleichzeitig beim Scannen verwendeten Threads

Das Ergebnis eines Discovery-Scanvorgangs für Netzwerke ist ein Bericht mit einer Liste aller gescannten Ziele und erkannten Dienste sowie zusätzlichen Informationen (abhängig von den verwendeten Optionen).

Falls mit dem Scan lediglich geprüft werden soll, ob der Host aktiv ist und nicht die Dienste, die er ausführt, kann der „Erkennungsmodus“ aktiviert werden. Das Scanverfahren in diesem Modus – für jeden Host im Gültigkeitsbereich – umfasst die ARP-Auflösung (in lokalen Segmenten), ICMP-PING und einen eingeschränkten Scan der Standardports für SSH-, HTTP-, HTTPS- und Remote-Desktop-Dienste. Wird bei einem von ihnen ein aktiver Host festgestellt, erfolgt eine entsprechende Markierung – danach geht es weiter mit dem nächsten Ziel.

Systemscans

Es handelt sich um einen netzwerkbasierten Schwachstellen-Scanner, der jedes System mit IP-Adresse auf häufig auftretende Schwachstellen hin untersucht.

Bei diesem Vorgang kommen sowohl aktive als auch passive Schwachstellenprüfungen zum Einsatz. So wird beispielsweise versucht, den Dienst (das Produkt) und seine Versionsnummer zu identifizieren. Sobald diese erkannt wurde, prüft der Systemscan, ob die jeweilige Software bekannte Angriffspunkte aufweist. Zusätzlich zur passiven, auf Banner-Grabbing basierenden Prüfung führt die Funktion auch aktive Analysen durch, um die Existenz bestimmter Defizite oder Systemfehlkonfigurationen zu bestätigen. Beim authentifizierten Scannen kann man auch fehlende Sicherheitspatches und veraltete Software aufspüren.

Hinweis: Systemscan arbeitet unterbrechungsfrei und ist so konzipiert, dass Ihre Systeme nicht den Dienst verweigern.

Beim Start des Features erfolgt zunächst ein Portscan des Ziels. Sobald alle offenen Ports (Dienste) erkannt worden sind, erfolgt die Untersuchung auf Schwachstellen. Hier folgt nur ein kleiner Teil der Systeme, die mit Systemscan beleuchtet werden können:

- Webserver
- Firewalls
- E-Mail-Server und -Gateways
- Router und Switches
- Domain Controller
- DNS-Server
- Antivirus-Gateways
- Workstations

Zu den vom Scanner ausgeführten Tests zählen:

- Erkennung von Diensten und Betriebssystemen (UDP/TCP/CMP)
- Prüfung auf Schwachstellen und Fehlkonfigurationen bei Diensten
- Prüfung auf Schwachstellen und Fehlkonfigurationen bei Betriebssystemen
- Prüfung auf Schwachstellen und Fehlkonfigurationen bei Netzwerkgeräten
- Prüfung auf sichere Konfigurationen (SSL/SSH)
- Identifizierung von Standardkennwörtern (Betriebssysteme, Dienste, Netzwerk, Geräte)

Alle Schwachstellen werden mit einem CVSSv2-Score, CVE, BID, BugTraq und anderen Referenzen gemeldet, sofern verfügbar.

Webscans

Mit diesem Feature können Sie Webanwendungen untersuchen und testen. Sie können Webscans auch im Rahmen der Entwicklung neuer Anwendungen einsetzen. Da Schwächen hier schon zu Beginn des Entwicklungsprozesses entdeckt werden, lassen sich Kosten und Anzahl der Ressourcen für eine spätere Bekämpfung erheblich reduzieren.

Webscan gilt als ergänzende Prüfung, die zusätzlich zu einem Systemscan-Vorgang durchgeführt werden kann. Es empfiehlt sich, dass Sie jedes Mal, wenn Sie ein Ziel mit Systemscan untersuchen, Systeme mit Webanwendungen ebenfalls mit Webscan prüfen.

Definition der Webscan-Ziele

Berücksichtigen Sie beim Definieren der Ziel-URL für einen Webscan, dass die automatische Site-Erkennung (Crawling und das, was tatsächlich gescannt wird) auf Standorte beschränkt ist, die:

- Die gleiche Portnummer wie das definierte Scanziel besitzen (das heißt: Port 80 – Standard für http://.., Port 443 – Standard für https://, Port 8080 – wenn ausdrücklich wie folgt spezifiziert: https://www.some-site.com:8080/).
- Das gleiche Protokoll wie das definierte Scanziel besitzen (mit anderen Worten: Wenn Sie die URL http://www.company.com angeben, wird mit dem Scan https://www.company.com nicht automatisch zusätzlich geprüft).
- Den gleichen FQDN wie das Scanziel haben (mit anderen Worten: Wenn Sie die URL https://service.com angeben, werden mit dem Scan nicht automatisch unter https://www.service.com verfügbare Inhalte geprüft).

Dies dient zum Schutz von Objekten, die der Kunde nicht überprüfen möchte. So kann es sich zum Beispiel bei **http://www.bank.com** um eine offizielle Website einer Bank mit allgemeinen Infos handeln. Andererseits kann **https://www.bank.com** ein Host für einen komplett unterschiedlichen Service sein, etwa für Onlinebanking. Der gleiche Webscan-Vorgang ist nicht notwendigerweise zur Prüfung beider gedacht.

Benutzerdefinierte Webanwendungen

Bevor Sie einen neuen Webscan erstellen, müssen Sie zunächst die Szenarien verstehen, in denen er wirksam ist. Als Faustregel gilt, dass Sie nur benutzerdefinierte Webanwendungen scannen sollten. Wenn auf einem System beispielsweise eine Standardausführung von WordPress (ohne benutzerdefinierte Module) läuft, ergibt es keinen Sinn, Webscan zu verwenden, da Systemscan die WordPress-Version und bekannte Schwachstellen identifizieren kann. Wenn Sie jedoch wissen, dass Ihre WordPress-Version speziell entwickelte Module enthält, sollten Sie sie sowohl mit Systemscan als auch mit Webscan prüfen. Beachten Sie dabei, dass Sie nur den benutzerdefinierten Code oder das benutzerdefinierte Modul scannen müssen und nicht die gesamte Website.

Wir verwenden beide – die Top 10 und die 55 statischen Kategorien

Webscan erkennt Sicherheitsdefizite in kommerziellen und benutzerdefinierten Webanwendungen und testet auf zahlreiche Schwachstellen, einschließlich der OWASP Top 10.

- Webanwendungsscanner, der Schwachstellen in benutzerdefinierten Anwendungen identifiziert
- Authentifizierung, die auf Formularen basiert
- Support für unterstütztes Crawling (Aufzeichnungen)
- Skalierbarkeit für kontinuierliches Wachstum
- Scan-Tool, das nach PCI ASV zertifiziert ist

Zusätzlich zu den Top 10 setzt F-Secure Radar auch die 55 statischen Kategorien der Bedrohungsklassifizierung ein, die vom Web Application Security Consortium (WASC) definiert wurden.

Mit ihr sollen unterschiedliche Sicherheitsrisiken für Websites herausgestellt werden. Die Mitglieder des WASC haben das Projekt zur Entwicklung und Förderung einer genormten Branchenterminologie erstellt. Anwendungsentwickler, Sicherheitsexperten, Softwareanbieter und Complianceprüfer sollen so Zugriff auf eine konsistente Sprache und Definitionen für Probleme im Zusammenhang mit der Websicherheit haben.

Scan Node Agent

Diese F-Secure-Radar-Komponente verwaltet alle auf dem Scanknoten ausgeführten Prüfprozesse.

Mit ihr werden alle Scanjobs überwacht (Liste aller Prüfungen mit System-, Web- und Erkennungsscan) und das Radar-Sicherheitscenter auf neue Scanjobs in der Warteschlange geprüft. Der Scanknoten verfügt über seine eigene Kapazität und weiß, wie viele Scans – je nach Konfiguration – gleichzeitig ausgeführt werden können.

Ist ein Scan abgeschlossen, sendet Scan Node Agent einen Bericht an das Security Center und löscht alle temporären Scandaten vom Knoten, einschließlich Scanbericht und -protokoll. Wichtig: Nach Abschluss des Scans erfolgt keine Speicherung von Schwachstellendaten auf dem Knoten. Es handelt sich um eine Komponente von Radar, die per Neuinstallation jederzeit ausgetauscht werden kann, wenn keine Scans laufen.

Scan Node Agent wird als Dienst im Betriebssystem ausgeführt und mit einer zusätzlichen Anwendung für Systemadministratoren ausgeliefert, mit der diese eine Vorschau der Konfiguration des Scanknotens und des Status von Scanjobs sehen können sowie Details der aktuell auf dem Knoten ausgeführten Scans.

Management

Auf der Seite „Account Management“ können Sie den Benutzerzugriff für Radar mithilfe von RBAC-Prinzipien (Role Based Access Control) steuern. Die Benutzerverwaltung in Radar umfasst drei Bereiche: Benutzer, Benutzergruppen und Rollen.

Benutzer

Die „Account Management“-Seite zeigt eine Liste aller Anwender an, die Zugriff auf Ihr Radar-Konto haben. Dort können Sie die User und deren Zugriff überprüfen und auch beliebig viele hinzufügen oder wieder entfernen.

Benutzergruppen

Benutzergruppen fungieren als Container für einen oder mehrere Benutzer. Mit ihnen können Sie steuern, auf welche Scangruppen User Zugriff bekommen und mit welchen Berechtigungen (Rollen). Die Spalte „User Groups“ zeigt an, zu welchen Gruppen die aufgelisteten Benutzer gehören.

Rollen

Mit Rollen können Sie Inhalte definieren, auf die ein User zugreifen kann. So lassen sich beispielsweise Rollen wie „View only“, „System owner“ und „Administrator“ erstellen. Um die Rollen für Ihr Radar-Konto anzuzeigen und zu bearbeiten, klicken Sie auf die Menüschaltfläche „Account Management“ und wählen dann „Manage roles“.

Berichterstattung

Die Berichterstattung ist ein weiterer äußerst wichtiger Bestandteil von Radar Security Centre. Mit Radar können Sie benutzerdefinierte Berichte erstellen, die den Anforderungen Ihres Managers, Systemadministrators oder Drittanbieters entsprechen.

Sie können auch eigene Berichte auf der Seite „Reports" generieren. Diese werden dann der Liste auf der Seite „Summary Reports" hinzugefügt. Sie können jeden Bericht in verschiedenen Formaten anzeigen:

- XML: Download von Rohdaten des Berichts im XML-Format.
- Nach Hosts gruppierter Word-Bericht, der alle technischen Details der Hosts im Scanbereich enthält, geordnet nach Host. Dies ist nützlich, wenn Sie für den Scan keine große Anzahl an Hosts definiert haben.
- Word-Bericht nach Schwachstellen geordnet: Details der Hosts im Scanbereich, geordnet nach Art der Schwächen. So erhalten Sie einen übersichtlichen Bericht, wenn der Scanbereich sehr groß ausfällt.
- Excel-Bericht nach Schwachstellen gruppiert, der alle technischen Details der Hosts im Scanbereich abdeckt. Ermöglicht die Nutzung der in Excel verfügbaren Funktionen.
- Zusammenfassung als Word-Bericht: Als kompakte Berichterstattung mit wenigen Seiten konzipiert, selbst wenn die Zusammenfassung Tausende von Hosts überblickt.

Hinweis: Nach der Erstellung eines Berichts wird eine Momentaufnahme Ihrer Schwachstellen angelegt. Um den Bericht zu aktualisieren, klicken Sie auf das Menüsymbol in der Spalte „Actions" und wählen dann „Refresh report data". „Create a new report" benutzen Sie hingegen, wenn Sie die vorhandene Dokumentation nicht überschreiben möchten.

WERTVERSPRECHEN

Strategisch

Schützen Sie Ihre Marke indem Sie Zwischenfälle verhindern

Bleiben Sie regelkonform (z. B. PCI DSS)

Sicherheit ist gleich Qualität und gilt für jedes Angebot

Taktisch

Sicherheitsmanagement

Ausführung

Fähigkeiten zur Erkennung von Schwach-stellen zum Schutz Ihrer Systeme

Entwicklung von sicheren Anwendungen

Mehr Einblick in Ihre Umgebungen

Zu den größten Ängsten von Firmen zählen Rufschädigung, schlechte Presse und Vertrauensverlust aufgrund von Inkompetenz oder Fahrlässigkeit. Zu den weiteren möglichen Folgen gehören Produktivitätseinbußen, der Verlust von Wettbewerbsvorteilen durch den Diebstahl wichtigen geistigen Eigentums sowie potenzielle Richtlinienverstöße im Zusammenhang mit der DSGVO.

Sie brauchen Einblicke in die Schnittmenge zwischen den Schwachstellen Ihrer Umgebungen und den Sicherheitslücken, die in freier Wildbahn ausgenutzt werden. Darüber hinaus müssen Sie dabei denjenigen Schwachstellen höchste Priorität einräumen, die die größten Risiken für Ihr Unternehmen darstellen.

Umfassendes Bedrohungsmanagement mit F-Secure Radar

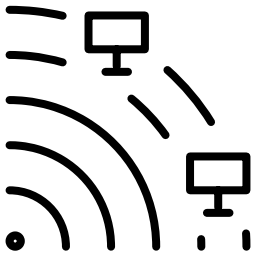
Bei F-Secure Radar handelt es sich um eine von der F-Secure Corporation entwickelte Plattform für das Scannen und Managen von Sicherheitslücken. F-Secure Radar ist wahlweise als cloudbasierter Service (SaaS) oder lokale Lösung erhältlich. Radar besteht aus folgenden Komponenten:

- Radar Scan Nodes
- Radar Security Center

Mit Scan Nodes erfolgt der eigentliche Scan. Das Security Center verwaltet und koordiniert die Scanknoten, erstellt Berichte und sammelt Ergebnisse.

F-Secure Radar erkennt Schwachstellen sofort und erhöht so die Netzwerk- sowie Anwendungssicherheit. Zudem gewährleistet Radar die Einhaltung gesetzlicher Vorschriften. Das Sicherheitsmanagement lässt sich durch eine erstklassige zentrale Berichterstellung und eingehende Analysen effektiv verbessern.

F-SECURE RADAR



Umfassende Transparenz

Wirksames Sicherheits-Mapping durch präzise Erfassung und Zuordnung aller Assets, Systeme und Anwendungen innerhalb des Netzwerks und darüber hinaus.

Optimiertes Produktivitäts- und Sicherheitsmanagement

Beseitigung von Problemen über mehrere Domains hinweg per effizientem Workflow. Inklusive Schwachstellenüberwachung, automatischen Scans und Ticketing-System für die priorisierte Behebung von Schwachstellen.

Effizientes Sicherheitsmanagement

Vereinfachte Integration mit einem nützlichen Service-Workflow- und Ticketing-System, das Schwachstellen mit planbaren Scans überwacht. Priorisiertes Patching und Zuweisung der Koordination durch Systemadministratoren (zum Beispiel ServiceNow).

Risikoberichte

Berichte mit zuverlässigen Informationen zur Sicherheitlage Ihrer Firma über die Zeit. Demonstrieren Sie, wie IT-Sicherheit geschäftliche Kontinuität gewährleistet.

Geringere Kosten

Mit Schwachstellen-Management können Sie Ihre Sicherheitskosten deutlich senken. Es ist kosteneffizienter, sich mit Sicherheit auseinanderzusetzen, bevor es zu schwerwiegenden Problemen kommt, als später wertvolle Zeit und Ressourcen für die Krisenbewältigung zu verschwenden. Darüber hinaus bieten die Cloud-Ressourcen von Radar eine weitere Möglichkeit für Einsparungen.

Erfüllung aktueller und zukünftiger Gesetzesrichtlinien

F-Secure Radar erfüllt als PCI ASV die Anforderungen für das Scannen von Schwachstellen. Als Ihr kompetenter Partner in der EU garantieren wir die Einhaltung von allen relevanten Vorschriften. Indem Sie F-Secure Radar verwenden, gewährleisten Sie die Compliance mit einer zugelassenen PCI-ASV-Scanlösung beziehungsweise PCI-Konformität mit einem QSA-Partner (Qualified Security Assessor). Führen Sie regelmäßige Tests durch und erkennen Sie neue Schwachstellen. Generieren Sie benutzerfreundliche Berichte für alle Beteiligten.

ÜBER F-SECURE

Niemand hat einen besseren Einblick in echte Cyber-Angriffe als F-Secure. Wir schließen die Lücke zwischen Erkennung und Reaktion. Zu diesem Zweck nutzen wir die konkurrenzlosen Informationen über Bedrohungen von Hunderten der besten technischen Berater unserer Branche, Millionen von Geräten, die unsere preisgekrönte Software nutzen, sowie fortlaufenden Innovationen im Bereich Künstliche Intelligenz. Führende Banken, Fluggesellschaften und Unternehmen vertrauen auf unser Engagement bei der Bekämpfung der gefährlichsten Bedrohungen der Welt.

Zusammen mit unserem Netzwerk an Top-Channel-Partnern und über 200 Serviceanbietern ist es unsere Mission, all unseren Kunden maßgeschneiderte unternehmensfähige Cyber-Sicherheit zur Verfügung zu stellen. F-Secure wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd gelistet.

f-secure.com | twitter.com/fsecure | linkedin.com/f-secure

F-Secure