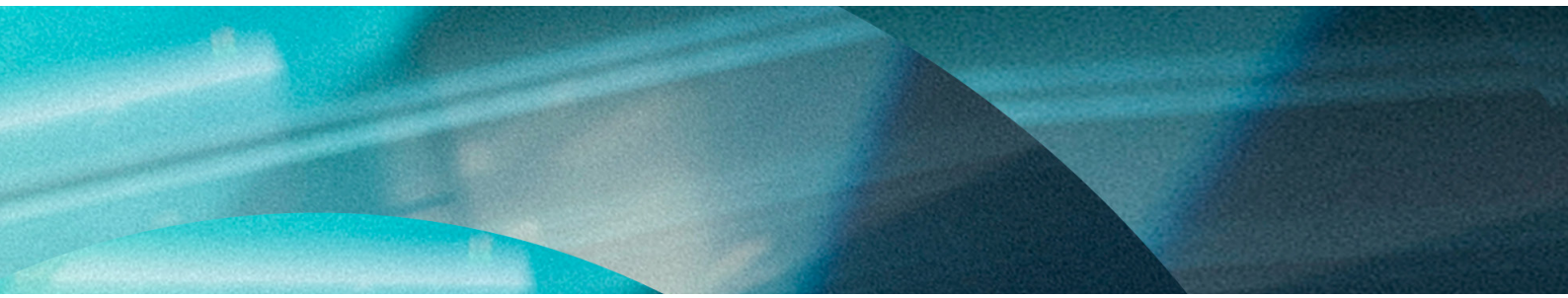
Vulnerability Management

– brauchen wir das?

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE



Schwachstellen in Software und Hardware zählen zu den größten Bedrohungen der IT-Sicherheit eines Unternehmens. Diese Lücken muss man natürlich beseitigen, aber das Löcherstopfen als simpler Reflex greift am Ende zu kurz. Besser ist ein umfassendes Schwachstellenmanagement, das Risiken und Systeme nach Dringlichkeit gewichtet und Notfallpläne parat hält.

Die IT-Landschaft eines Unternehmens ist in der Regel heterogen aufgebaut und besteht aus Produkten ganz unterschiedlicher Hersteller. In vielen Firmen kommen noch Hunderte von Tools und Programmen hinzu, die von den Mitarbeitern oder Fachabteilungen an der zentralen IT vorbei in Eigenregie heruntergeladen und eingerichtet werden. Auf Desktop-PCs, Notebooks, Smartphones und Tablets entsteht so ein Wildwuchs von Apps und Anwendungen, den die Administratoren nicht mehr kontrollieren können. Dazu kommt noch die große Zahl an Servern, Betriebssystemen und Anwendungen, die von der IT bereitgestellt werden.

Aufgrund der hohen Komplexität moderner Software und Hardware weisen viele dieser Produkte mehr oder weniger kritische Sicherheitslücken auf. Die Vulnerability-Database (VulDB[1]) zum Beispiel enthielt bei Redaktionsschluss Anfang Juni 2020 insgesamt 153.710 Verweise auf Sicherheitslücken. Der Berichtszeitraum erstreckt sich dabei bis zurück ins Jahr 1970. Im Jahr 2020 kamen bislang 7836 Einträge hinzu, das entspricht durchschnittlich 50,23 pro Tag. Außerdem wurden seit Jahresanfang durchschnittlich 134,26 Einträge täglich überarbeitet, sei es, weil ein Patch veröffentlicht worden oder weil beispielsweise ein neuer Exploit bekannt geworden war.

[1] **VulDB:** Stats (https://vuldb.com/?stats) [Stand: 5. Juni 2020]. Vergleichbare Datenbanken gibt es auch auf https://nvd.nist.gov, https://exploit-db.com oder https://cvedetails.com.

Gefahrenabwehr muss automatisierbar sein.

Die Zahl der bekannten und neu entdeckten Schwachstellen ist damit viel zu groß, als dass eine IT-Abteilung sie zeitnah eingehend analysieren könnte. Dasselbe gilt für die von den Herstellern veröffentlichten Patches und Updates, die getestet und installiert werden müssten. Bewältigen lässt sich diese Aufgabe nur mithilfe einer weitgehenden Automatisierung. Es gibt heute bereits Tools, die nicht nur den Bestand der Software und Hardware im Unternehmensnetzwerk erfassen. Diese Programme verfolgen auch die Meldungen zu neu gefundenen Schwachstellen und Sicherheitslücken und weisen die Administratoren darauf hin, wenn dadurch Gefahren für das Netzwerk des Unternehmens entstehen.

Ein Beispiel ist cyberscan.io[2] von der Deutschen Gesellschaft für Cybersicherheit. Das Programm untersucht automatisch die aus dem Internet erreichbaren Assets einer Organisation oder eines Unternehmens auf bekannte Schwachstellen und verweist dann, sofern sie verfügbar sind, auf Fixes und Patches sowie die zugehörigen Download-Adressen.

Zu den „Wirtschaftsgütern" von Unternehmen zählt man in der IT die Hardware und Software wie Desktop-Computer, Server, Netzwerke, aber auch Smartphones, Tablets, virtuelle Maschinen, Container oder IoT-Geräte. Eine Lösung, die all diese Endpunkte in das Vulnerability Management einbezieht, ist zum Beispiel Tenable.Die Frage ist nur, ob das ständige Patchen, Fixen und Updaten tatsächlich eine langfristig tragfähige Lösung ist. Oder ob dieser reaktive Ansatz nicht etwas zu kurz greift. Bei diesen Überlegungen müssen IT-Abteilungen berücksichtigen, dass zwischen dem Erkennen einer Schwachstelle und der Verfügbarkeit eines Patches oder Updates, je nach Dringlichkeit und Gefährlichkeit, immer einige Tage, wenn nicht sogar Wochen oder Monate verstreichen. In dieser Zeit sind die Unternehmenssysteme angreifbar, während in der kriminellen Hackerszene schon Anleitungen kursieren, wie sich die Lücke ausnutzen lässt. Um das Unternehmen unter diesen Bedingungen so gut wie möglich vor Datendiebstahl, Datenverlusten und Erpressungsversuchen per Ransomware zu schützen, ist daher ein weiter gefasstes Konzept erforderlich.

[2] **Deutsche Gesellschaft für Cybersicherheit:** cyberscan.io (https://www.cyberscan.io).

Patch Management:
Flicken ist gut, heilen wäre besser.

Für die Verteilung von Patches im Unternehmen ist ein Patch Management notwendig. In seiner klassischen Form umfasst es die Organisation der Verteilung von Patches und Updates auf die Systeme der Firma, und zwar so, dass die Bandbreite im Netzwerk möglichst wenig belastet wird. Zum Patch Management gehören die Information über neu bekannt gewordene Schwachstellen und verfügbare Fixes, die Beschaffung der Software, Tests auf Funktionsfähigkeit, die Priorisierung der zu versorgenden Systeme, die Installation und schließlich die Dokumentation. Vieles davon lässt sich über Tools oder selbst geschriebene Skripte automatisieren. Dennoch ist das Patch Management in den meisten IT-Abteilungen aufgrund der Vielzahl der neu veröffentlichten Fixes und Updates und des damit verbundenen Arbeitsaufwands eine ungeliebte Aufgabe.

Die Alternative ist ein Schwachstellen- oder Vulnerability Management. Es verfolgt einen übergeordneten Ansatz. Denn das Verteilen der Patches allein genügt oft nicht, um die Sicherheit der Assets des Unternehmens und die Funktion der IT zu gewährleisten. Ein Beispiel: Wenn sich beim Test eines neuen Patches herausstellt, dass er bei der speziellen Konfiguration eines Servers entweder keinen Schutz bietet oder sogar die Funktion der Software einschränkt, ist die Frage zu klären, ob der Fix überhaupt installiert werden soll oder ob es vielleicht andere Möglichkeiten oder Workarounds gibt. Diese Überlegungen sind dann Aufgabe des Vulnerability Managements, das über das reine Patch Management hinausgeht. Welche Aufgaben es außerdem noch umfasst, wird im Folgenden erläutert.

Vulnerability Management:
Laufend am Geschäft ausgerichtet.

Um den Unterschied zwischen Patch Management und Vulnerability Management zu verdeutlichen, ist vielleicht der folgende Hinweis hilfreich: Das Patch Management ist üblicherweise Aufgabe der IT-Abteilung, während das Vulnerability Management eher in den Aufgabenbereich der Security-Abteilung fällt. Der Prozess sieht dann folgendermaßen aus: Die Security identifiziert eine Schwachstelle bei einem der IT-Assets der Firma und erzeugt ein Ticket für die IT-Abteilung, damit diese die Sicherheitslücke schließt. Sobald das geschehen ist, gibt die IT eine Meldung über den Erfolg der getroffenen Maßnahme, etwa die Installation eines Patches, zurück. Eine Definition könnte etwa so aussehen:

Vulnerability Management ist ein kontinuierlicher Prozess, der die vorhandene Software und Hardware im Netzwerk erfasst, die Betriebssysteme und Anwendungen kategorisiert, Berichte zu den bekannten Sicherheitslücken zusammenstellt und mögliche Lösungswege erarbeitet.

Da jeden Tag Dutzende neuer Schwachstellen und Sicherheitslücken bekannt werden, muss das Vulnerability Management logischerweise ein ständig aktiver Prozess sein. Dabei muss das Unternehmen regelmäßig Scans und Analysen durchführen, um auf Grundlage der jeweiligen Bedrohungslage das eigene Risiko einzuschätzen. Das bedeutet, dass die Berichte der Patch-Management-Software und eventueller Penetrationstests kontinuierlich ausgewertet und auf die IT-Infrastruktur im Unternehmen bezogen werden müssen.

Gleichzeitig müssen die mit dem Vulnerability Management betrauten Mitarbeiter aber auch vorausschauend aktiv werden: Auf der Basis von Analysen, die zum Beispiel die besonders kritischen Abschnitte im Unternehmensnetzwerk definieren, stellen sie Strategien auf, wie sich diese Bereiche schützen lassen, wenn eine Sicherheitslücke bekannt wird – auch dann, wenn noch keine Patches und Updates vorliegen. (Einige gangbare Wege werden weiter unten im Text aufgezeigt.) Ähnliche Analysen sollten die Fachleute für alle besonders gefährdeten Bereiche der IT-Landschaft zusammenstellen. Hierzu zählen zum Beispiel Remote-Steuerungen, Onlineshops, Backup-Server oder Content-Management-Systeme. Nur wenn solche Pläne bereits vorbeugend ausgearbeitet worden sind, kann die IT-Abteilung schnell reagieren, falls das Bedrohungsrisiko plötzlich ansteigt – zum Beispiel, weil eine bisher unbekannte Sicherheitslücke entdeckt worden ist.

Phase 1:
Netzwerkinfrastruktur scannen, einmal und immer wieder.

Das Schwachstellenmanagement beginnt mit einem Scan: Mithilfe einer Software wie Tenable oder eines anderen Programms erfasst das Unternehmen in einem ersten Schritt die vorhandenen Assets. Diese Scans folgen einem festen Ablaufplan:

1. Zunächst sucht die Software nach allen Systemen, die über das Netzwerk erreichbar sind. Zu diesem Zweck sendet sie Pings und TCP/UDP-Pakete aus.
2. Im zweiten Schritt identifiziert sie die offenen Ports und laufenden Dienste auf den Computern.
3. Falls möglich, loggt sich die Software ein und fragt detaillierte Systeminformationen ab.
4. Schließlich gleicht sie die Systeminformationen mit bekannten Schwachstellen ab.

Es ist wichtig, dass die Scansoftware so viele Daten wie möglich sammelt, bei Hardware-Assets also beispielsweise die Modellnummer und die genau Firmware-Version, bei Software die Versionsnummer und die eingespielten Updates und Patches. Nur wenn diese Übersicht vollständig und genau ist, kann ein passendes Sicherheitskonzept für das Unternehmen entworfen werden. Diese Scans müssen außerdem regelmäßig wiederholt und ihre Ergebnisse müssen mit den bereits erfassten Daten verglichen werden.

Denn zum einen sind nie sämtliche Assets eines Unternehmens gleichzeitig aktiv, ein Teil davon wird also bei einem einmaligen Scan gar nicht erfasst. Dazu zählen unbesetzte Arbeitsplätze genauso wie Server und virtuelle Maschinen, die gerade gewartet werden, aber auch ausgeschaltete Peripheriegeräte wie Drucker oder Scanner. Zum anderen versorgen viele Hersteller ihre Geräte und Anwendungen regelmäßig und ohne Zutun der Anwender mit Updates und Fixes. Diese Änderungen sollte das Vulnerability Management immer sofort berücksichtigen.

Weil die Scans regelmäßig wiederholt werden, sollten sie automatisch ablaufen. Dasselbe gilt für die Aktualisierung der Ergebnisse. Oft wird es dennoch nötig sein, einige Objekte, die von der Scan-Software nicht identifiziert werden konnten, von Hand nachzutragen, etwa Legacy-Hardware oder Tools, die im Unternehmen entwickelt worden sind. Das ist normalerweise aber nur in der Aufbauphase eines Vulnerability Managements notwendig.

Die Scans erfüllen noch eine zweite Funktion. Sie sollten nämlich nicht nur die von den Herstellern gelieferten Informationen auswerten, sondern im Rahmen eines Penetrationstests Netzwerk und Anwendungen auch auf Fehlkonfigurationen und eventuell sogar auf bislang unbekannte Sicherheitslücken untersuchen. Zu den Fehlkonfigurationen zählen beispielsweise versehentlich offengelassene Ports, ein Rechtemanagement, das den Anwendern Vollzugriff auf geschützte Ordner erlaubt, oder die Möglichkeit zur Wahl unsicherer Passwörter. Auch ein unbeschränkter Zugriff auf Hardware-Ressourcen wie Drucker, Router, Webcams oder IoT-Geräte gehört in diese Kategorie.

Neuere Ansätze beim Vulnerability Management versuchen dabei, die Zahl der Netzwerkscans so gering wie möglich zu halten, um die verfügbare Bandbreite nicht unnötig zu belasten. In diesem Fall lassen Administratoren die Software gezielt nur die neu angeschlossenen Geräte scannen und deren Daten in die zentrale Datenbank aufnehmen, ohne dafür die komplette Umgebung ein weiteres Mal einzulesen. Teilweise arbeiten die Systeme heute auch mit Software-Agenten, die ständig aktuell Software-Versionen und Hinweise auf bekannte Verwundbarkeiten und Patches liefern, ohne dass dafür ein Scan angestoßen werden müsste.

Auch ein kontinuierlicher Scan der aus dem Internet erreichbaren Server (Webserver, Outlook Web Access, Mail-Server, FTP-Server etc.) muss erfolgen. Hier ist die Gefahr, dass eine Sicherheitslücke ausgenutzt wird, sogar noch wesentlich höher. Denn meist kann auf diese Server unbeobachtet aus der gesamten Welt zugegriffen werden. Dies stellt ein sehr großes, fast unkalkulierbares Risiko dar. Die Server werden zwar bei einem Penetrationstest überprüft, aber dieser wird, wenn überhaupt, nur alle zwei bis drei Jahre durchgeführt. Somit können der IT-Abteilung gar nicht alle aktuellen Sicherheitslücken bekannt sein. Hierbei hilft zum Beispiel cyberscan.io in dem es auch diese Scans aus dem Internet automatisiert und dann die IT-Abteilung automatisch benachrichtigen kann.

Phase 2:
Den Bestand mit Schwachstellen-katalogen abgleichen.

In der zweiten Phase geht es darum, die Assets zu kategorisieren. Das geschieht etwa nach Betriebssystemen, Clients, Arten von Anwendungen, physischen und virtuellen Servern, Abteilungen, privater und geschäftlich genutzter Hardware etc. Die Wahl der Kategorien sollte sich nach den Gegebenheiten im jeweiligen Unternehmen richten.

Als Nächstes erfolgt der Abgleich des Verzeichnisses mit einem Dienst oder einer Datenbank wie der oben vorgestellten Vulnerability-Database. Auch diese Aufgabe lässt sich mit einem geeigneten Software-Paket automatisieren, und auch bei diesem Schritt werden oft Nacharbeiten von Hand erforderlich sein. Zunächst einmal geht es darum, zu prüfen, welche Assets bei Patches und Updates auf dem neuesten Stand sind und welche nicht. Gleichzeitig erfahren Administratoren durch den Abgleich aber auch, bei welchen Geräten, Servern oder Anwendungen Sicherheitslücken bekannt sind, für die es noch keine Patches gibt – eine Information, die für das weitere Vorgehen oft entscheidend ist. Zu den weiteren Fragen, die geklärt werden sollten, gehört aber auch:

- Wie schwierig wäre es, die Schwachstelle auszunutzen?
- Gibt es bereits bekannte Exploits, die die Schwachstelle angreifen?

Dieser Datenabgleich muss ebenfalls kontinuierlich aktualisiert werden, da die Hersteller ständig Patches und Updates veröffentlichen und sich die Gefährdungslage dadurch von einem Tag auf den anderen ändern kann.

Phase 3:
Risikozonen bestimmen, Baustellen priorisieren.

Der nächste Schritt unterscheidet das umfassendere Schwachstellenmanagement wesentlich vom reinen Patch Management. Ausgangspunkt ist die Überlegung, dass nicht alle IT-Assets eines Unternehmens gleichermaßen sicher sein müssen. Für einen Desktop-PC beispielsweise, der ausschließlich Dokumente auf einem zentralen Fileserver bearbeitet, gelten verhältnismäßig geringe Sicherheitsanforderungen. Ein Backup-System hingegen, das im Falle eines Ransomware-Angriffs überlebenswichtig ist, verlangt dagegen ein sehr hohes Level an Sicherheit.

Im Rahmen des Vulnerability Managements ist es daher notwendig und hilfreich, die Assets des Unternehmens zu priorisieren: Was ist am wichtigsten? Was ist weniger wichtig? Die Reihenfolge orientiert sich an den jeweiligen Sicherheits- und Geschäftszielen des Unternehmens. Zu klären sind dabei Fragen wie diese:

- Welche Abteilungen sind für das Unternehmen und/oder die Aufrechterhaltung der Produktion besonders wichtig und müssen daher vorrangig geschützt werden?
- Welche Server, Datenbanken, Backup-Systeme etc. enthalten Daten, die für das Unternehmen existenziell sind?
- Gibt es Netzwerkabschnitte, in denen unternehmenskritische Daten und/oder Anwendungen zusammengefasst sind?
- Welche Systeme sind für die wichtigsten drei Geschäftsprozesse am wichtigsten?

Diese Fragen kann die IT- oder Security-Abteilung nicht allein beantworten. Es ist unumgänglich, dass an diesem Punkt die Geschäftsführung einbezogen wird. Sobald die Grundlagen jedoch geklärt sind, lässt sich daraus die Priorität für den Schutz der Daten und Systeme ableiten. Die IT-Abteilung ist dann in der Lage zu definieren, welche Systeme beispielsweise beim Verteilen von Patches und Updates vorrangig versorgt werden.

Umgang mit Assets:
Was sofort drankommt (und was egal ist).

Damit ergibt sich dann auch, welche Software- und Hardware-Hersteller die IT-Abteilung besonders im Blick behält, wenn es um neue Verwundbarkeiten oder die Bereitstellung von Updates geht. Darüber hinaus lässt sich aus der Liste auch ableiten, bei welchen Computern oder Software-Installationen die Patch-Dringlichkeit am höchsten ist. Erscheint beispielsweise ein sicherheitskritisches Update für Microsoft Windows, ist es insbesondere für größere Unternehmen hilfreich, wenn sie auf Basis der Priorisierung einen Plan für die Installation auf den Desktop-Rechnern entwickelt haben.

Des Weiteren kann die IT-Abteilung festlegen, wie vorzugehen ist, wenn bei einem System Schwachstellen bekannt werden, die der Hersteller selbst nicht beheben wird – zum Beispiel weil die Firma nicht mehr existiert oder weil die Software aus dem Support gelaufen ist. In einem solchen Fall wäre es bei einem unternehmenskritischen System mit hoher Priorität notwendig, es durch ein neues, besser abgesichertes System mit Support-Vertrag zu ersetzen. Eine andere Möglichkeit der Lösung bestünde darin, rund um das System eine demilitarisierte Zone (DMZ) aufzubauen, also ein durch Firewalls oder eine Air Gap geschütztes, isoliertes Computernetz. Des Weiteren gibt es auch verschiedene „virtuelle" Patching-Möglichkeiten. Indem man zum Beispiel den Datenverkehr zu den Systemen mit den Sicherheitslücken aktiv überwacht, lässt sich feststellen, ob im Netzwerkverkehr gerade ein Angriff verübt wird, der diese Schwachstellen ausnutzt. Ein virtuelles Patching kann sich ebenso in virtuellen Umgebungen anbieten. So lassen sich durch Schnittstellen in den Hypervisor-Plattformen auch die dort laufenden virtuellen Server oder Clients aktiv überwachen.Viele Angriffe auf bekannte Sicherheitslücken lassen sich außerdem mittels eines IPS (Intrusion Prevention Systems) oder IDS (Intrusion Detection Systems) feststellen. Diese sind meist Teile einer Firewall und helfen auch bei einer Netzwerktrennung weiter.

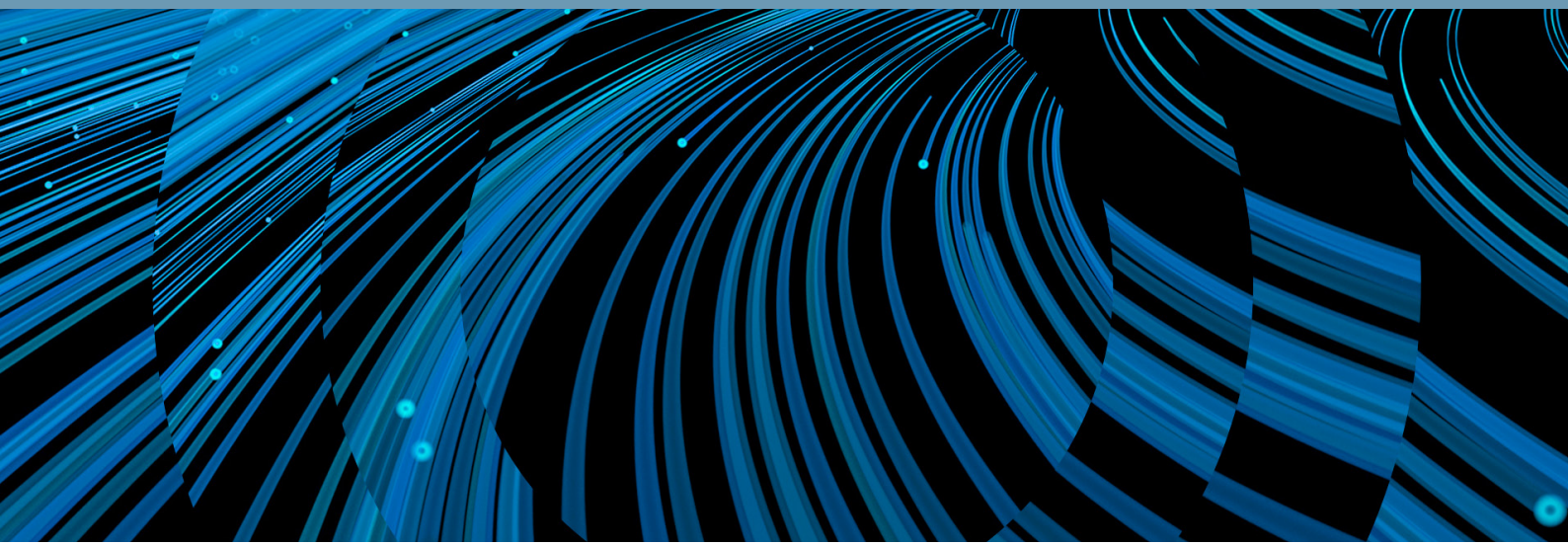
Auf der anderen Seite lässt sich bei der Sortierung nach Dringlichkeit auch festlegen, dass auf bestimmten Systemen überhaupt nicht oder nur in größeren Intervallen Updates eingespielt werden, beispielsweise auf Systemen, auf die von außen gar kein Zugriff möglich ist. Vulnerability Management bedeutet immer auch, Schwachstellen bei Assets, die für das Unternehmen wenig wichtig sind, zu ignorieren oder nachrangig zu behandeln. Das ist etwa dann sinnvoll, wenn das Schließen einer Sicherheitslücke teurer käme als der Schaden, den ein Angreifer verursachen könnte.

Darüber hinaus kann die IT präventiv weitere Maßnahmen festlegen. So kommt es immer wieder vor, dass in der Software eines unternehmenskritischen Systems eine Sicherheitslücke entdeckt wird, für die der Hersteller jedoch noch keinen Patch bereitstellen kann. Ein geeigneter Notfallplan könnte dann vorsehen, das System in dieser Situation vom Netzwerk zu trennen, um das Risiko eines Datendiebstahls zu minimieren. Oft finden sich auch Workarounds, zum Beispiel könnte man die betroffenen Daten auf einen anderen, sicheren Server übertragen, vorübergehend in die Cloud auslagern oder die Zugriffsberechtigungen strikt einschränken. Eine gute Strategie kann es auch sein, die Wahrscheinlichkeit zu verringern, dass jemand die Schwachstelle ausnutzt. Auf diese Weise gewinnt das Unternehmen Zeit für die Suche nach einer Abwehrmöglichkeit.

Umgang mit Lücken:
Was hochriskant ist (und was uns nicht betrifft).

Ein weiterer wichtiger Punkt besteht darin, das Gefahrenpotenzial einer neu bekannt gewordenen Schwachstelle zu analysieren.

Denn oft genug ist es durch die spezielle Konstellation von Software und Hardware, wie sie im Unternehmen eingesetzt wird, überhaupt unmöglich, dass ein krimineller Hacker die Sicherheitslücke für seine Zwecke ausnutzt. Manche Sicherheitslücken stehen nur dann offen, wenn das jeweilige Asset direkt mit dem Internet verbunden ist. Andere lassen sich nur bei Einsatz eines bestimmten Protokolls ausnutzen, wieder andere treten nur in Verbindung mit einer bestimmten Konfiguration eines Programms oder einer Firmware auf. Es ist die Aufgabe des Vulnerability Managements, zu untersuchen, ob im Unternehmen die Bedingungen tatsächlich gegeben sind, dass Angreifer eine bestimmte Lücke ausnutzen. Falls nicht, ist das Einspielen des Patches oder Updates weniger dringlich. Die IT muss also folgende Punkte klären:



- Lässt sich das Asset, bei dem die Schwachstelle bekannt ist, vom Internet aus ansprechen?
- Wie schwierig wäre es, diese Schwachstelle auszunutzen? (Genügen vielleicht schon nicht genug geschulte Anwender, die leichtgläubig den Anhang einer E-Mail öffnen?)
- Gibt es andere Sicherheitsmechanismen, die die Wahrscheinlichkeit verringern, dass die Schwachstelle ausgenutzt wird?
- Wie lange ist die Schwachstelle bereits bekannt und wie lang ist das betroffene System bereits im Firmennetzwerk aktiv?

Es gibt Fälle, in denen Unternehmen nur 3 % der Schwachstellen bei ihrer Software und Hardware beseitigen mussten, um gegen Angriffe weitgehend gefeit zu sein. Das ist das Ziel des Vulnerability Managements: Das Risiko mithilfe von Scans und Analysen so stark einzugrenzen, dass es mit verhältnismäßig geringem Aufwand beherrschbar ist.

Vulnerability Management:
Wie kann Bechtle dabei helfen?

Setzen Sie sich einfach mit uns in Verbindung und erfahren Sie mehr zum Thema oder über unsere vielen Services und Lösungen rund um das Thema IT-Security:

security.ls@bechtle.com

Schwachstellenmanagement ist sowohl bei der Planung und Einrichtung wie auch später in der Praxis ein relativ aufwendiger Prozess. Trotz Automatisierung binden Analysen, Priorisierungen und Pläne ein oder mehrere IT-Mitarbeiter. Wenn der zuständige Administrator bereits etwas Erfahrung mit dem Thema gesammelt hat, gelingt eine effiziente Lösung am besten. Doch gerade bei vielen mittelständischen Unternehmen ist das Fachpersonal knapp, es fehlt an Know-how und Ressourcen für den geordneten Umgang mit IT-Risiken.

Bechtle bietet seinen Kunden daher ein effektives Schwachstellenmanagement inklusive Unterstützung bei Konzeptionierung, Planung, Implementierung und praktischem Betrieb einer Vulnerability-Management-Lösung an. Gemeinsam mit dem Anwenderunternehmen klären die Experten von Bechtle die konkreten Anforderungen und führen erste Scans zur Bestandsaufnahme und zur Einschätzung des Gesamtrisikos durch. Selbst bei Systemen mit Schwachstellen, für die kein Patch oder Update verfügbar ist, hilft Bechtle bei der Lösung, etwa durch die sichere Einrichtung einer DMZ. Außerdem kann Deutschlands größtes IT-Systemhaus auch Software anbieten, die das Netzwerk des Unternehmens im Hintergrund regelmäßig und automatisch auf Verwundbarkeiten testet, den Erfolg der Maßnahmen mit Einzeltests der Assets überprüft und gezielt die Einhaltung von gesetzlichen Security-Richtlinien und -Empfehlungen überwacht.

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE