

Schwachstellenmanagement mit dem GSM

Inhalt

- Vulnerability Assessment
- Vulnerability Management
- Wo beginnt man und wie hoch ist das Risiko?
- Die Steuerung der Scan-Engine

Einleitung

Schwachstellenmanagement (engl. Vulnerability Management) bietet einen echten Mehrwert bei der Organisation der IT-Sicherheit im Allgemeinen und dem präventiven Härten von IT-Systemen gegen erfolgreiche Angriffe seitens Innen- und Außentätern im Besonderen.

Um den Mehrwert des Schwachstellenmanagements zu entfalten muss es aber in einen Sicherheits-Prozess eingebunden werden. Dem Erkennen der Schwachstellen muss die Beseitigung (Update, Patch oder Rekonfiguration) oder die Behandlung über einen anderen Sicherheitsmechanismus (IDS, Firewall-Regel) folgen. Durch Schwachstellenmanagement werden für die System-Administration Schwachstellen erkannt. Für das IT-Management wird ein hilfreiches Werkzeug zum Risiko-Management sowie Compliance und Qualitätsmonitoring für die IT-Sicherheit angeboten.

Vulnerability Assessment

Unter "Vulnerability Assessment" versteht man das Erkennen von Schwachstellen in IT-Systemen.

Diese können durch Fehlkonfiguration oder Programmierfehler entstehen.

Durch das Vulnerability Assessment werden diese festgestellt und dokumentiert. Durch einen Patch oder eine Re-Konfiguration werden diese Schwachstellen abgestellt. Sollte eine Re-Konfiguration nicht möglich sein, kann durch Vorkehrungen wie Firewall-Regel oder eine sog. "Intrusion Prevention"-Regel diese Schwachstelle zumindest entschärft werden.

Vulnerability Management

Nachdem die Schwachstellen erkannt wurden, sind diesbezügliche Informationen in einen Management-Prozess einzubetten. Dieser Prozess wird als "Vulnerability Management", also Schwachstellenmanagement, bezeichnet.

Durch diesen Prozess wird eine Dokumentation des Sicherheitsstatus bzw. Änderung des Sicherheitsstatus und Benchmark der Sicherheit ermöglicht. Durch das Überführen der Scan-Ergebnisse in den Management-Prozess ist es möglich mit einfachen Kennzahlen oder Ampeln aufzuzeigen, ob Schwachstellen existieren, ob sie zwischenzeitlich von der IT-Administration geschlossen wurden oder ob neue

Schwachstellen im Rahmen des fortlaufenden Vulnerability Assessments aufgedeckt wurden.

Patchen ersetzt kein Vulnerability Management

Selbst für sorgfältig gepatchte Systeme ist weiterhin ein ebenso sorgfältiges Vulnerability Management notwendig.

Zum einen ist es aufgrund von System-Abhängigkeiten oft nicht möglich einen aktuellen Patch-Level einzupflegen, da ansonsten spezielle Datenbank- oder sonstige unternehmenskritische Applikationen nicht mehr ausgeführt werden kann bzw. die Zertifizierung verliert.

Zum anderen muss beachtet werden, dass für manche Schwachstellen kein Patch existiert, oder Schwachstellen trotz aktuellem Softwarestand durch reine Fehlkonfiguration erzeugt werden können. Ein Administratoren-Passwort "12345678" ist ein klassisches Beispiel, ein weiteres sind Dateisystem-Freigaben welche aus Versehen in das Internet geöffnet werden.

Schwachstellen-Scans allein reichen nicht, Handeln ist nötig

Die Sicherheit einer IT-Infrastruktur wird nicht allein dadurch verbessert, dass alle Schwachstellen durch Vulnerability Assessment erfasst und dokumentiert werden. Die Schwachstellen sind immer über einen Organisationsprozess durch die jeweiligen Verantwortlichen weiter zureichen.

Begleitend ist ein Management-Prozess aufzubauen, welcher die weitere Verfolgung der Schwachstellen mit ggf. auch Technologie- oder Management-Konsequenzen garantiert. Auch die Gegenmaßnahmen sind in diesem Prozess zu dokumentieren und auf die technische Wirksamkeit zu prüfen. Dieses kann durch einen erneuten Vulnerability Assessment Scan oder durch einen detaillierten Test mit einem anderem Software-Werkzeug erfolgen.

Ein verwundbarer Dienst welcher nicht für einen Kerngeschäftsprozess notwendig ist, kann zeitweise oder komplett abgeschaltet werden oder durch eine Firewall bzw. IPS-Regelsatz abgesichert werden. Durch Dokumentation mit Kontrolle und Beobachtung von verwundbaren Diensten können solche ebenfalls abgesichert werden, wenn er durch sonstige Alternativen nicht geschützt werden kann. Beispielsweise kann eine Log-Regel in der Firewall Nachweis über einen berechtigten und unberechtigten Zugriff auf potenziell verwundbare Systeme dokumentieren und Angriffsvorwürfe entkräften.

Schwachstellenmanagement wird nicht rein technisch gelöst

Die Basis eines erfolgreichen Schwachstellenmanagement sind die Organisationsprozesse welche die technischen Erkenntnisse vom Vulnerability Assessment in einen Arbeitsprozess überführen, der zur Schließung der Schwachstellen führt. Dabei müssen je nach Risiko der System-Administration geeignete Werkzeuge zur Verfügung gestellt werden um diesen Sicherheitsprozess abzubilden.

Ebenso muss die technische IT-Abteilung mit Mitteln versehen werden um die erkannten Schwachstellen zu schließen oder wenigstens zu entschärfen. Auch geeignete Sicherheitsrichtlinien, welche eine Fehlkonfiguration zu vermeiden helfen, sind über einen Organisationsprozess abzubilden.

Organisatorischer Rahmen von Schwachstellenmanagement und Sicherheitsrichtlinien

Im Rahmen des Organisationsprozesses können Prüfungen der Richtlinien in Greenbone Prüf-Skripte überführt werden. Die damit schließlich automatisierte Prüfung auf Einhaltung der Sicherheitsrichtlinien (im englischen "Compliance") bedeutet eine erhebliche Arbeitserleichterung.

Wo beginnt man und wie hoch ist das Risiko?

Es hat sich in der Praxis als hilfreich erwiesen dort zu beginnen wo das operative Risiko am höchsten ist.

Dieses Risiko kann durch ein konzern-eigenes Risiko-Management System ermittelt werden. Für weniger komplexe Anforderungen kann auch eine einfache Faustformel benutzt werden:

$$\text{Risiko} = \text{Bedrohungs-Wahrscheinlichkeit} * \text{Möglicher Schaden}$$

Dies lässt sich auch auf die einzelnen bekannt gewordenen Schwachstellen (hier: S) beziehen:

$$\text{Risiko(S)} = \text{Bedrohungs-Wahrscheinlichkeit(S)} * \text{Möglicher Schaden(S)}$$

In diesem Fall setzt sich die die Bedrohungs-Wahrscheinlichkeit konkret aus dem Bedrohungs-Szenario und dem Schwachstellen-Schweregrad zusammen. Das Bedrohungs-Szenario beschreibt, wie einfach es für einen Angreifer ist die Schwachstelle auszunutzen. Also:

$$\text{Risiko(S)} = \text{Bedrohungs-Szenario(S)} * \text{Schwachstellen-Schweregrad(S)} * \text{Schaden(S)}$$

Das Bedrohungs-Szenario eines Webservers in einer DMZ, und damit ans Internet angeschlossen, ist sicherlich höher, als das eines Webservers welcher nur über eine Telefon-Einwahlleitung erreichbar ist. Der Schaden an einer Produktions-Maschine ungleich höher, als der Verlust des firmeneigenen Webservers für Image-Filme.

Man erhält selbst mit stark vereinfachten Kategorien für Bedrohungs-Szenario, Schwachstellen-Schweregrad und Schaden ein Kennziffer die bereits eine Priorisierung erlaubt wo man mit der Arbeit beginnen sollte. Der Schwachstellen-Schweregrad wird für jede Schwachstelleninformation bereits mitgeliefert. Man muss also nur noch das Bedrohungs-Szenario und den Schaden einer Kategorie zuordnen.

Neues Tool, neues Risiko

Dabei ist zu beachten, dass auch jedes neue IT-Sicherheitswerkzeug ein inhärentes Risiko mit sich bringt.

Solche Software-Werkzeuge können den Geschäftsbetrieb beeinträchtigen da diese an empfindlichen und sicherheitsrelevanten Stellen eingesetzt werden. Auch können Schwachstellen in solch einer Software schnell selbst zu einem Sicherheitsrisiko werden.

Manche Schwachstellen-Scanner benötigen das Administratoren-Passwort für die Domäne, quasi einen Generalschlüssel. Dabei ist nicht klar was die Scan-Software damit alles noch tätigt, oder gar ob dieses über eine Hintertür böseartig oder auch nur für Wartungszwecke Unbefugten zugänglich werden könnte

Zentralistische Lösungen sind ineffektiv und bringen zusätzliche Risiken

Der Kern eines Schwachstellen-Scanners ist die sog. "Scan-Engine". Bei einigen Anbietern wird sie zentral in deren Rechenzentrum betrieben. Die bei den Kunden platzierten Scan-Appliance macht einen sog. "Layer-2 Tunnel" zwischen dem eigenen IT-Netz, dem Ziel des Scanners, und dem Datacenter des Scan-Anbieters auf.

Dann werden alle Informationen zu gefundenen Schwachstellen über ein Web-Portal via Internet zugänglich gemacht.

Es ist oft vertraglich schwer oder gar nicht nachvollziehbar wo die Informationen über die Schwachstellen der eigenen Firma abgelegt werden. In vielen Fällen werden sie auf zentralen Servern in den USA oder Indien abgelegt. Eine solche Konzentration bekannter Schwachstellen stellt ein außerordentlich attraktives Ziel und eine begehrliche Datenquelle für Insider-Angriffe dar.

Aus Sicht des Risiko-Management ist kaum einsichtig, dass in sensiblen Infrastrukturen solche Tunnel eingebracht werden, und dann alle Schwachstellen außerhalb der betrieblichen Richtlinien und kontrollierbaren Bereiche abgelegt werden. Weder auf das Löschen noch auf die Archivierung hat der Kunde einer solchen Lösung einen unmittelbaren Einfluss. Betriebliche Richtlinien zur Kontrolle der IT-Bereich haben einen sehr realen Hintergrund bekommen: Bei Online-Auktionshäusern wie z.B. Ebay lassen sich aus Insolvenzen stammende oder einfach nur ausgemusterte Festplatten aus verschiedenen Rechenzentren erwerben. In der Regel sind die Daten restaurierbar, falls überhaupt eine Löschung durchgeführt wurde.

Wenn im Gegensatz dazu die Scan-Engine komplett auf einer Appliance im eigenem Rechenzentrum des Unternehmens betrieben wird, dann bedeutet dies einen gewissen Mehraufwand an Pflege der Scan-Engine. Gewonnen wird aber bei der Sicherheit, denn die operativen und betrieblichen Risiken werden durch Eliminierung von Unwägbarkeiten gesenkt.

Proprietäre Lösungen sind intransparent

Das Alleinstellungsmerkmal des Greenbone Security Manager ist seine beweisbare und unabhängig prüfbare Sicherheit. Da die komplette Scan-Engine und alle Prüfroutinen im Quelltext als Open Source zur Verfügung stehen können sie durch Kunden und Dritte vollumfänglich auditiert werden.

Wo proprietäre Lösungen Marketing-Versprechen und -Beteuerungen anbieten setzt Greenbone auf Fakten die durch jede dritte Partei im Vertrauen des Kunden verifiziert werden können.

Durch die Öffnung des gesamten Prozesses kann der Kunde das Risiko bei dem Einsatz des Greenbone Security Managers besser abschätzen. Die transparente Scan-Engine bietet bewiesene Sicherheit und das Abonnement der tagesaktuelle Prüfroutinen die Aufdeckung der meisten relevanten Schwachstellen sowie unmittelbare Einsicht in die technischen Testverfahren.

Die Steuerung der Scan-Engine

Den Kern des Greenbone Security Managers (GSM) bilden die Scan-Engine und ein Steuerungsmodul für diese Scan-Engine. Das Steuerungsmodul verwaltet die Datenbank und erlaubt die Verwendung der GSM Appliance über verschiedene Benutzerschnittstellen.

Je nach Anwendungszweck kann man flexibel die Art der Steuerung und Verwaltung wählen.

Fernsteuerbar via Kommandozeile (CLI)

Durch einen CLI-Client (CLI steht für Command Line Interface) ist es möglich, verschiedene Scan-Aufgaben über Skripte oder eine Zeitsteuerung (z.B. CRON-Dämon) periodisch automatisch auszuführen, und somit eine komplette fernsteuerbare Integration in ein spezialisiertes unternehmenseigenes System einzufügen. Der Sicherheitsstatus und dessen Änderung sowie die eigentlichen Scan-Ergebnisse können dann via XML-Ausgabe in ansprechende Berichte überführt werden.

Desktop-Client für Experten

Für Sicherheitsexperten steht ein sog. "Desktop-Client" zur Verfügung. Diese Graphische Benutzeroberfläche ermöglicht es, sehr komplexe bzw. feinkörnige Scan-Konfigurationen zu erstellen.

Das sehr umfangreiche Experten-Werkzeug wird vor allem von Auditoren und Sicherheits-Spezialisten verwendet.

Web-Oberfläche Greenbone Security Assistant (GSA)

Damit der GSM schon aus dem Stand heraus ohne weitere Installation von Software (eine häufige Anforderung von KMUs) über den Webbrowser eingesetzt werden kann, hat Greenbone Networks den Greenbone Security Assistant entwickelt und zu einem festen Bestandteil des GSM gemacht..

Die intuitive Web-Oberfläche bietet die Verwaltung von Benutzern, Scans mit daraus resultierenden Berichten, Scan-Konfigurationen, Ziel-Konfigurationen und Zugangsdaten.

Scan-Profile lassen sich vom Desktop-Client auf den GSA importieren und somit spezielle Prüfungen auch weniger technisch versiertem Personal oder dem Management zur Verfügung stellen.

Der GSA zeigt auf einfache Weise den Sicherheitsstatus und dessen Trend via Web-Oberfläche an.

Ein PDF, HTML und XML Export von dem Report ist mit wenigen "Clicks" einfach zu erreichen.

Status: 20091120