Deloitte.

Enterprise Risk Services

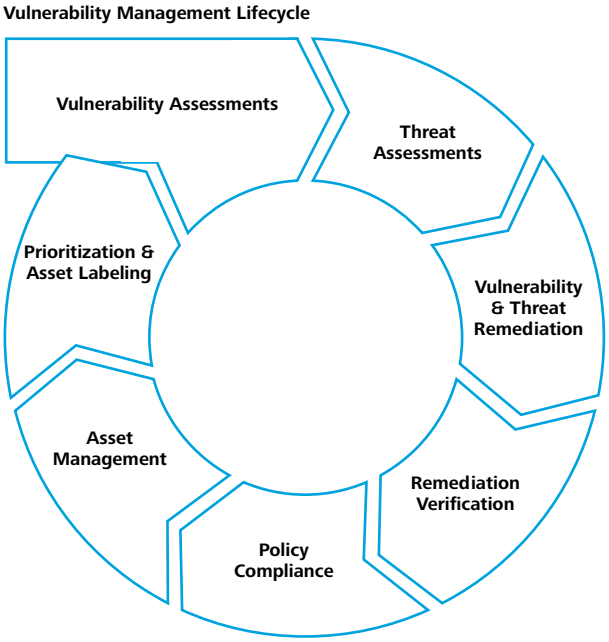
Vulnerability Management
Ist Ihr Unternehmen geschützt?

Was ist Vulnerability Management (VM)?
Das VM beschäftigt sich mit der Identifikation und Behebung von Verwundbarkeit in der IT-Infrastruktur. Hierdurch können Risiken für die IT-Infrastruktur reduziert und das Sicherheitsniveau nachhaltig verbessert werden. Ziel ist die präventive Erkennung und Behebung von Schwachstellen – noch bevor diese durch eine Cyber-Attacke ausgenutzt werden können. Denn nur wer seine Schwächen kennt, kann sich effektiv schützen.

Wie funktioniert Vulnerability Management?
Das VM zentralisiert diverse – meist schon vorhandene – Aktivitäten. So werden beispielweise regelmäßige Sicherheitsuntersuchungen durch das VM initiiert, die Ergebnisse im Businesskontext evaluiert und notwendige Maßnahmen daraus abgeleitet. Auch die Kontrolle der umgesetzten Maßnahmen auf ihre Effektivität gehört in vielen Organisationen zum Aufgabenbereich des VM.

Bestandteile des modernen Vulnerability Management

Zu den Methoden des VM gehören als Hauptbestandteile:



Ein Teil hiervon, der häufig fälschlicherweise als VM betrachtet wird, ist das Patch Management, das mit in die Vulnerability & Threat Remediation fällt. Wenn es um Software-Schwachstellen geht, können diese zwar meist mit Hilfe von Patches geschlossen werden, allerdings gibt es viele andere Arten von Schwachstellen, wie beispielsweise menschliches Versagen oder Organisationsschwächen, die durch entsprechende Maßnahmen wie Mitarbeiterschulungen, Prozessanpassungen und Konfigurationsänderungen zu adressieren sind.

Zusätzlich zu den klassischen Bestandteilen gehört eine Vielzahl von Verlinkungen zu anderen Sicherheitsprozessen wie beispielsweise dem Security Incident Handling. Die durch das VM gewonnenen Informationen helfen im Incident-Fall, das konkrete Risiko sowie Schadenpotenzial schneller und genauer zu ermitteln.

Typische Probleme beim Vulnerability Management

Die richtigen Maßnahmen werden falsch angewandt

Es werden regelmäßige Sicherheitsuntersuchungen durchgeführt, die Ergebnisse aber nicht messbar gemacht und keine strategischen Maßnahmen erarbeitet, um ähnlichen Schwächen in Zukunft vorzubeugen.

Der Irrglaube, Vulnerability Management sei ein rein technisches Problem

Schwachstellen entstehen auch aus zu schwachen oder fehlenden Policy-Vorgaben sowie einem mangelnden Sicherheitsbewusstsein von Mitarbeitern. Genauso müssen identifizierte Schwächen, wenn immer möglich, strategisch angegangen werden und nicht rein per technischer Lösung, will man eine anhaltende Verbesserung erzielen.

Schwächen, die ohne Gesamtkontext betrachtet werden

Eine einzelne identifizierte Schwachstelle mag auf den ersten Blick kaum relevant erscheinen. Im Gesamtkontext jedoch kann sie eine kritische Rolle spielen.

Sich nicht vor noch unbekannten Schwächen schützen

Meist wird penibel darauf geachtet, nicht von bekannten Angriffsarten und Malware verwundbar zu sein. Taktische und strategische Maßnahmen, die auch gegen noch unbekannte Bedrohungen und Cyber-Attacken schützen, werden dann häufig vernachlässigt.

Warum Deloitte?

- Weltweit über 12.000 Mitarbeiter im Bereich Security & Privacy, davon über 1.100 CISSPs (Certified Information Systems Security Professionals) – mehr als in jeder anderen Service-Organisation.
- Strategisches Vorgehen basierend auf aktuellen Standards und den Erfahrungen von zahlreichen IT-Sicherheitsprojekten.
- Aktive Mitwirkung in Organisationen, die sich mit IT-Sicherheit befassen: Information Security Forum (ISF), Informations Systems Audit & Controls Association (ISACA), International Information Systems Security Certification Consortium (ISC)², Information Systems Security Association (ISSA), CyLab, I-4, IAPP, American Society for Industrial Security (ASIS), International Standards Organization (ISO) und Open Web Application Security Project (OWASP).
- Breite und Tiefe von Fachwissen und Fähigkeiten – wir verfügen über umfassendes und detailliertes Fachwissen. Dies ermöglicht es uns, alle Anforderungen an ein angemessenes VM in Ihrer Organisation umzusetzen.
- Praktische Umsetzungserfahrung – wir haben Erfahrung in der Entwicklung komplexer Sicherheitsprogramme, in denen Menschen, Prozesse und technologischer Wandel ganzheitlich betrachtet werden.
- Ausgezeichnete Projektmanagementfähigkeiten – Deloitte setzt seine langjährige und umfangreiche Erfahrung im Projektmanagement wirksam ein, um Ihren Projektaufwand zu reduzieren.
- Gemeinschaftliche Herangehensweise – für Deloitte hat die enge Zusammenarbeit mit Kunden und deren Partnern hohe Priorität und stellt einen wichtigen Baustein für den Erfolg der Projekte dar.

Unsere Leistungen

Deloitte verfügt über ein Spezialistenteam, das Sie von der Aufnahme und Bewertung Ihrer Assets, der Überprüfung Ihres aktuellen Sicherheitsniveaus mit Erarbeitung sicherheitssteigernder Maßnahmen bis hin zum angestrebten Sicherheitslevel sowie Ihren Compliance-Zielen unterstützt.

Mit einem erprobten und auf Ihr Unternehmen maßgeschneiderten sowie in Ihre Gegebenheiten integrierbaren VM-Lösungsansatz führt Deloitte zu einer umfassenden und anhaltenden Erhöhung der Sicherheit gegen Cyber-Attacken und hilft, die vorhandenen Schwachstellen und daraus resultierenden Risiken in den Griff zu bekommen.

Hierbei wird anhand eines speziell entwickelten Kennzahlensystems die Grundlage geschaffen, den Reifegrad Ihrer Prozesse und Methoden zu bestimmen und Veränderungen in der Sicherheit messbar zu machen.

Wir helfen Ihnen, ein angemessenes VM in Ihrem Unternehmen zu integrieren, sowie bei der Ausgestaltung sämtlicher Bestandteile, um ein möglichst effizientes, proaktives und anhaltendes Management Ihrer potenziellen Schwächen sicherstellen zu können.

Ihre Ansprechpartner

Für mehr Informationen
Peter J. Wirnsperger
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Für weitere Informationen besuchen Sie unsere Webseite auf
www.deloitte.com/de/cyber

Stand 05/2013