Systeme • Netzwerke • Sicherheit

Informationen zur Durchführung eines m-bit Sicherheitsscans

1. - Präambel

Dieser Text orientiert sich am BSI (Bundesamt für Sicherheit in der Informationstechnik) Dokument „Ein Praxis-Leitfaden für Penetrationstests“ Version 1.0 vom November 2014, der auf www.bsi.bund.de verfügbar ist.

Schwachstellenscans können niemals eine 100%ige Aussage über den Zustand eines Prüfobjekts machen: erstens gilt die Heisenbergsche Unschärferelation, zweitens werden Schwachstellenscans immer mit einer zeitlichen und damit monetären Obergrenze beauftragt. Im Gegensatz dazu haben wirkliche Angreifer eine quasi unbegrenzte Menge Zeit, so dass reale Angriffe u.U. Wochen und Monate andauern können. Weiterhin werden laufend neue Schwachstellen ausgelotet, dokumentiert und benutzt, so dass eine Prüfung nur einen Schnappschuss der Situation wiedergibt. Sicherheit ist kein Produkt, sondern ein Prozess.

2. - Einleitung

Im folgenden Dokument geben wir Ihnen einen Überblick über die Arten und Optionen der von der Firma m-bit durchgeführten Arten und Module von Schwachstellenscans. Kein Kunde gleicht einem anderen und keine EDV oder Netzanbindung gleicht einer anderen. Weil das so ist, bieten wir einem Kunden unterschiedliche Vorgehensweisen und Möglichkeiten eines Schwachstellenscans an. Der Aufwand für einen Scan ist in erster Linie von der Arbeitszeit des oder der Prüfer(s) abhängig, und hat damit direkten Einfluss auf die Prüftiefe. Bei der Durchführung eines Schwachstellenscans besteht immer die Möglichkeit von Störungen oder Systemabstürzen. Je größer die Prüftiefe, desto größer ist das Risiko von Störungen oder Systemabstürzen. Es gilt also, ein für den Kunden individuell passendes Verhältnis von Aufwand, Kosten, Prüftiefe und Risiko zu finden.

3. - Zielsetzung

Ein Schwachstellenscan dient normalerweise der:

- Erhöhung der Sicherheit der technischen Systeme
- Erhöhung der Sicherheit der organisatorischen Infrastruktur
- Identifikation von Schwachstellen

m-bit • Hellmuth Michaelis
Hallstraße 20
25462 Rellingen
UStID: DE295105592

Telefon: +49 (0)4101 / 85 299 - 20
Telefax: +49 (0)4101 / 85 299 - 21
E-Mail: info@m-bit.net
Web: https://m-bit.net

Um diese Ziele zu erreichen, wird nach Abschluss der Prüfung eine Dokumentation erstellt, die folgende Bestandteile enthält:

- Dokumentation des Prüfablaufs
- Aufzählung der bei der Prüfung gefundenen Besonderheiten
- Risikobewertung der einzelnen Besonderheiten
- Maßnahmenvorschläge zur Verbesserung der Sicherheit
- ggf. Prüfprotokolle und Ausdrucke

4. - Varianten

Wir unterscheiden grob drei Arten eines Sicherheitsscans, wobei Aufwand, Kosten, Prüftiefe und Risiko variieren. Alle Varianten können durch Module ergänzt werden oder es können auch Module übersprungen werden.

a) Variante „*technisches Sicherheitsaudit*“

Bei dieser Variante wird anhand der Versionen der eingesetzten Systeme und Anwendungen sowie den Konfigurationen auf mögliche Schwachstellen hingewiesen. Der Prüfer bedient die Anwendungen und Systeme hierbei nicht selbst, sondern lässt sich von einem Administrator vor Ort zeigen, welche Software-Versionen in welcher Konfiguration eingesetzt werden und welche Härtungsmaßnahmen getroffen wurden. Es wird anhand der vorgefundenen Versionen der Softwaresysteme und der umgesetzten Sicherheitsmaßnahmen auf mögliche Schwachstellen geschlossen. Der Aufwand ist moderat, das Risiko von Störungen ist minimal, die Prüftiefe ist gering.

b) Variante „*nicht-invasiver Schwachstellenscan*“

Dies ist die am meisten durchgeführte Art eines Scans, da sie eine gute Balance zwischen Kosten, Risiko und Nutzen darstellt. Der Prüfer scannt mit eigenen Geräten im zu prüfenden Netzabschnitt nach Schwachstellen. Hierzu werden u.U. mehrere Schwachstellenscanner eingesetzt; die ggf. gefundenen Schwachstellen werden so gut wie möglich dokumentiert, aber nicht ausgenutzt. Das Risiko von Störungen und Systemabstürzen ist gering, es kann aber nicht ausgeschlossen werden, das es zu Störungen und Systemabstürzen kommt. Die Prüftiefe ist für viele Szenarien ausreichend hoch. Die Ausgaben der Schwachstellenscanner müssen händisch geprüft und ggf. überarbeitet und/oder kommentiert werden.

c) Variante „*invasiver Schwachstellenscan*“

m-bit • Hellmuth Michaelis
Hallstraße 20
25462 Rellingen
USt-ID: DE295105592

Telefon: +49 (0)4101 / 85 299 - 20
Telefax: +49 (0)4101 / 85 299 - 21
E-Mail: info@m-bit.net
Web: https://m-bit.net

Zusätzlich zum nicht-invasiven Schwachstellenscan werden die hierbei gefundenen Schwachstellen ausgenutzt, um nicht autorisierten Zugriff auf Systeme und Anwendungen zu erlangen. Das geschieht durch Programme, die eigens zum Ausnutzen von bekannten Schwachstellen geschrieben wurden oder die während der Prüfung vom Prüfer geschrieben werden. Hierdurch wird letztlich nachgewiesen, dass ein System oder eine Anwendung tatsächlich angreifbar ist. Der Aufwand für diese Variante ist hoch, das Risiko von Störungen und Systemabstürzen ist hoch und die Prüftiefe ist hoch.

5. - Module/Bestandteile

Während einer Prüfung kommen die Module *Schwachstellenscanner* und ggf. *optionale Scanner* zum Einsatz. Ausserdem sind immer Programme wie „nmap“, „traceroute“ und „ping“ beteiligt. Für die Prüfung von http/https-Ports werden optional Programme wie „nikto“ und „OWASP zap“ zusätzlich hinzugezogen. Für bestimmte Anwendungsfälle kommen u.U. noch andere Werkzeuge sowie von m-bit selbst erstellte Programme zum Einsatz.

Schwachstellenscanner

- Portscanner (scannt auf zugreifbare TCP/UDP-Ports)
- Protokollscanner (z.B. TCP 3-Wege-Handshake)
- UDP/ICMP-Scan
- Protokollscanner SMTP, HTTP, SSH, DNS, SNMP, etc.
- kommerzielle und/oder freie Scanner (Nessus, OpenVAS)

optionale Scanner

- Protokollscanner IPSEC (Protokoll AH, ESP bzw. Port 500/4500)
- Anwendungsscanner (z.b. Webserver wie apache Module, Versionen von Libraries, Zugreifbarkeit im / in das Filesystem, etc.)

m-bit • Hellmuth Michaelis
Hallstraße 20
25462 Rellingen
UStID: DE295105592

Telefon: +49 (0)4101 / 85 299 - 20
Telefax: +49 (0)4101 / 85 299 - 21
E-Mail: info@m-bit.net
Web: https://m-bit.net

Informationen zur Durchführung eines m-bit Sicherheitsscans

Diese optionalen Module werden nur auf Wunsch des Kunden eingesetzt.

„menschliche“ Scanner	• Prüfung auf konzeptionelle Schwachstellen • Sicherheitsbegehungen (physische Sicherheit) • Social Engineering

Die folgend gelisteten Module sind optional und werden nur auf expliziten Wunsch eines Kunden eingesetzt. Der Aufwand und das Risiko sind als hoch einzustufen.

„menschliche“ Scanner	• Prüfung von Telefonanlagen, Faxservern und/oder sonstige Telekommunikationseinrichtungen • Ausnutzen von Exploits, Einbruchsversuche auf Anwendungsebene • USB-Angriffe (und/oder CD-ROM's, Floppies, etc.) • „Man in the middle“ & Spoofing Attacken • DNS poisoning & redirecting • „Denial of Service“ Attacken • Netzwerk Traffic Analyse • Advanced Persistent Threats (APT) • reverse Engineering / Disassemblierung • Source Code Check
Wörterbuch-gestützte Scanner	• Passwortscanner (brute force) per Datenbank auf Applikationen
drahtlose Scanner	• WLAN, Ausleuchtung, Angreifbarkeit, verwendete Protokolle, Übergänge ins LAN • Bluetooth Angriffe • teilweise: - Angriffe auf Telefonanlagen und/oder sonstige Telekommunikationseinrichtungen
Überprüfung von Clients	• Awareness Maßnamen • Social Engineering • HTTP/HTTPS „drive by infection“ • Phishing Mail (siehe auch APT, Social Engineering)

6. - Durchführung

m-bit • Hellmuth Michaelis
Hallstraße 20
25462 Rellingen
USt!D: DE295105592

Telefon: +49 (0)4101 / 85 299 - 20
Telefax: +49 (0)4101 / 85 299 - 21
E-Mail: info@m-bit.net
Web: https://m-bit.net

Informationen zur Durchführung eines m-bit Sicherheitsscans

Die Durchführung von Prüfungen hat den Ablauf:

1. **Informationsgewinnung**
   Es werden Informationen über das zu prüfende Objekt in allgemein zugänglichen Quellen gesucht und überprüft. Dies sind in der Hauptsache Netzinformationen, Routing-Informationen, DNS-Informationen, Informationen über die Firma und über die Mitarbeiter des Kunden - kurz: jede Information, die später dabei helfen könnte, unberechtigten Zugang zu Einrichtungen des Kunden zu erlangen.

2. **Prüfung**
   Während der Prüfung kommen die technischen Hilfsmittel zum Scan der beteiligten Netzabschnitte zum Zuge. Der Kunde muss in die Lage versetzt werden, die Prüfung jederzeit abbrechen zu können oder bestimmte Prüfprozeduren zu überspringen: dazu muss während der Prüfung eine reibungslose und unmittelbare Kommunikation zwischen Prüfer und Kunde etabliert sein. Oft ergeben sich während einer Prüfung Situationen, in der der Prüfer den Prüfablauf verändern möchte (mehr oder weniger tief testen), weil bestimmte Besonderheiten gefunden wurden. Dies wird unmittelbar mit dem Ansprechpartner beim Kunden besprochen und ggf. umgesetzt.

3. **Berichterstellung**
   Nach der Prüfung erstellt der Prüfer den schriftlichen Bericht bzw. die Dokumentation des Prüfablaufs, erläutert Besonderheiten und Auffälligkeiten in den Phasen Informationsgewinnung und Prüfung, erstellt die Beschreibungen der Risikobewertungen und Vorschläge für Verbesserungsmaßnahmen. Als Anlage werden Prüfberichte und Logdateien aufgenommen und ggf. während der Prüfung erlangte Daten auf CD-ROM hinzugefügt.

4. **Präsentation**
   Ein sinnvoller - aber optionaler - Punkt ist die Präsentation der Ergebnisse, die der Prüfer dem Kunden vorstellt. Hierbei ist zu klären, ob Management und IT einen gemeinsamen Termin wahrnehmen oder zwei getrennte Termine. Nach der Präsentation der Ergebnisse ergibt sich meist eine Diskussion aller Beteiligten sowie weitere Erläuterungen des Prüfers zu einzelnen Themen des Prüfberichts.

m-bit • Hellmuth Michaelis
Hallstraße 20
25462 Rellingen
UStID: DE295105592

Telefon: +49 (0)4101 / 85 299 - 20
Telefax: +49 (0)4101 / 85 299 - 21
E-Mail: info@m-bit.net
Web: https://m-bit.net