

IT-Security-Management

IT-Security

Andreas Unterweger

Studiengang Web Business & Technology
FH Kufstein

Sommersemester 2020

- Vor einem Angriff
 - Ziel: Abschreckung und/oder Vorbeugung
 - Beispiel: Schilder mit Hinweis auf Bewegungssensoren bzw. Sicherheitsschulung für Mitarbeiter
 - Weitere Beispiele: Zäune, Schlösser, Sensoren, Kameras, Spamfilter
- Während eines Angriffes
 - Ziel: Erkennung und Abwehr
 - Beispiel: Virus wird von Virenschanner erkannt und infizierte Datei isoliert („unter Quarantäne gestellt“)
 - Weitere Beispiele: Einbruchserkennungs-/-vermeidungssystem
- Nach einem Angriff
 - Ziel: Schadensminimierung
 - Beispiel: Wiederherstellung aus Sicherung

- **Nicht nur** auf Rechner und Server, sondern auch auf
 - Fernseher („Smart TVs“)
 - Drucker (auch Kopierer)
 - Smartphones
 - „Smart Appliances“ (Kühlschränke, Heizungssteuerungen, Glühbirnen)
 - Bordcomputer im Auto
 - Spielekonsolen (im Firmenumfeld selten relevant)
 - ...
- Komplexe Hardware/Software weist Sicherheitslücken auf
- Wie absichern? (Auswahl)
 - Hardening
 - (Falls notwendig manuelle) Updates via Patchmanagement
 - Netzwerkseitige Abtrennung
 - Risikoeindämmung (vorbeugend, vgl. später)

- Rechteeinschränkung (vgl. später)
- Fehlerbehandlung in Anwendungen
 - Überprüfung auf Fehlerzustände
 - Kontrollierte Reaktion, z.B. Fehlermeldung
 - Aussagekräftige Fehlermeldungen sind hilfreich
 - Vermeidet unkontrollierte Programmfortsetzung (würde Preisgabe von Daten o.ä. ermöglichen)
- Eingabeüberprüfung in Anwendungen
 - Benutzereingaben auf ungültige Daten überprüfen
 - Erlaubte Zeichen nach Bedarf einschränken
 - Unkontrollierte Ausführung von Benutzereingaben ist potenzielle Schwachstelle (z.B. über *Arbitrary Code Execution*)

Beispiel für mangelnde Eingabeüberprüfung

```
Command Prompt

C:\tmp1>md "T1&ping 8.8.8.8"
C:\tmp1>cd "T1&ping 8.8.8.8"
C:\tmp1\T1&ping 8.8.8.8>echo %CD%
C:\tmp1\T1

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=23ms TTL=45
Reply from 8.8.8.8: bytes=32 time=23ms TTL=45
Reply from 8.8.8.8: bytes=32 time=24ms TTL=45
Reply from 8.8.8.8: bytes=32 time=23ms TTL=45

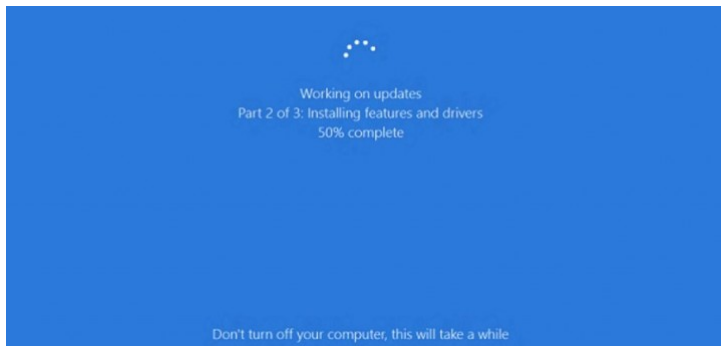
Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 24ms, Average = 23ms

C:\tmp1\T1&ping 8.8.8.8>
```

Quelle: The Security Factory: Command-injection vulnerability for COMMAND-Shell Scripts. <https://www.thurrott.com/windows/windows-10/66096/upcoming-build-windows-10-redstone-includes-refined-update-progress-ux> (Zugriff am 26.3.2017), 2017.

Patchmanagement

- Vorgehensweise, um bekannte Sicherheitslücken stopfen
- Ziel: Angriffsfläche minimieren
- Betrifft **alle** Anwendungen inkl. Betriebssystem
- Häufig: Erzwungene automatische Updates (z.B. monatlich)

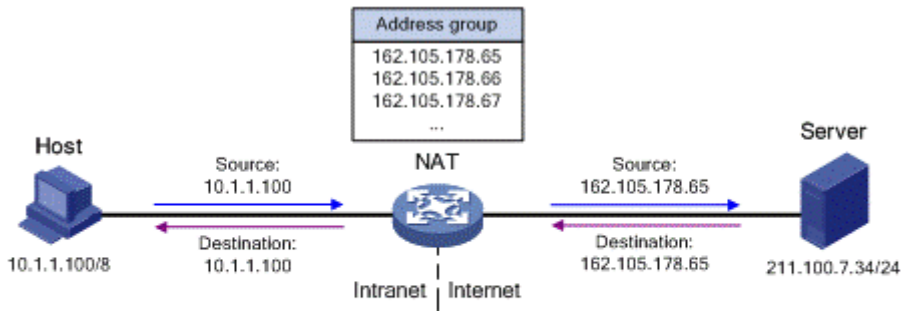


Adaptiert von Sams, B.: Next Build of Windows 10 Redstone Includes Refined Update Progress UX. <https://www.thurrott.com/windows/windows-10/66096/upcoming-build-windows-10-redstone-includes-refined-update-progress-ux> (Zugriff am 26.3.2017), 2016.

Netzwerkseitige Abtrennung zur Vorbeugung I

- Hauptziel: Kritische Infrastruktur weitestgehend isolieren
- Nebenziel: Frühzeitige Erkennung/Vermeidung von Angriffen
- Auf Layer 1/2 (Auswahl)
 - Switches statt Hubs verwenden (kein Mitlesen möglich)
 - MAC-Adressfilterung (unbekannte MAC-Adressen sperren)
 - Spezialhardware zur Erkennung von ARP Spoofing
 - Virtuelle LANs (VLANs): Logische Gruppierung von Rechnern unabhängig vom physischen Standort bzw. ihrer Switchzugehörigkeit
- Auf Layer 3 (Auswahl)
 - Kritische Hardware in eigenen (Sub-)Netzen
 - Router mit Firewallfunktion (Routen in kritische Netze stark einschränken, z.B. basierend auf Absenderadresse oder -netz)
 - **Network Address Translation (NAT)**: Verwendung privater IP-Adressen im Firmennetz mit eigener öffentlicher IP-Adresse (manchmal auch mehrere) nach außen → verschleiert Originaladressen

- Paketadressen werden durch Router ersetzt → Zuordnungsspeicherung



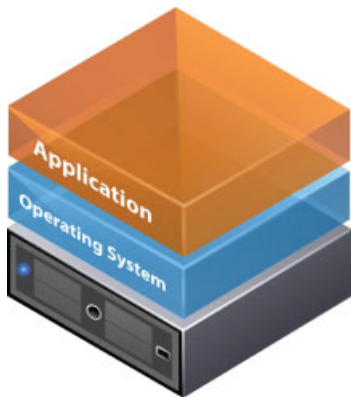
→ Packet from Host to Server

→ Packet from Server to Host

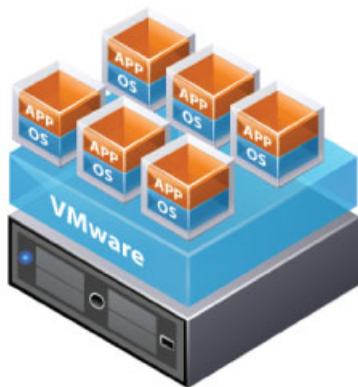
| NAT table | | |
|-----------|----------------|----------------|
| Way | Before NAT | After NAT |
| Outbound | 10.1.1.100 | 162.105.178.65 |
| Inbound | 162.105.178.65 | 10.1.1.100 |

Quelle: H3C Technologies: NAT Technology White Paper. http://www.h3c.com.hk/Products___Technology/Technology/Security_and_VPN/Technology_White_Paper/200808/613642_57_0.htm (Zugriff am 26.3.2017), 2017.

- Auf Layer 4 (Auswahl)
 - Firewalls mit festen Regeln (z.B. offene Ports für bestimmte Protokolle)
 - Firewalls mit *stateful packet inspection* (Untersuchung von Paketen mit Zustandsinformation, z.B. bisher gesendeten Daten)
- Auf Layer 7 (Auswahl)
 - Proxies (Anfragen über stellvertretendes Gerät senden und empfangen)
 - Spamfilter (unerwünschte Emails erreichen Mitarbeiter nicht)
 - Webfilter (Blockierung unerwünschter Seiten bzw. Inhalte)
- „Über“ Layer 7 (Auswahl)
 - Zugriffseinschränkung auf Router und andere Netzwerkgeräte (z.B. durch Passwörter und Adressfilterung)
 - Protokollierung von Zugriffen, blockierten Paketen etc. → Reaktion?
 - **Virtualisierung** (Abkapselung von Diensten in virtuellen Maschinen → Isolation mit einfachen Sicherheits- und Austauschmöglichkeiten)



Traditional Architecture



Virtual Architecture

Quelle: Virtual Networks: Cut IT Costs with Server Virtualization.

<http://www.virtualnetworks.co.za/index.php/virtualization/> (Zugriff am 26.3.2017), 2016.

- Engl. *Intrusion Detection Systems* (IDSs)
- Laufende Überwachung des Netzwerkes und der Dienste
- Überwachungskategorisierung
 - Anomalieerkennung (erfasst Abweichung von der „Norm“)
 - Signaturerkennung (wie Antivirenprogramm – sucht nach charakteristischen Mustern für bekannte Angriffe)
 - Verhaltenserkennung (wie Anomalieerkennung, aber adaptiv)
- Systemkategorisierung
 - Hostbasiert: Läuft auf Server oder Rechner und überwacht Dateisystem, Systemprozesse etc.
 - Netzwerkbasierend: Erkennt ungewöhnliche Pakete im Netzwerk
- Erweiterte Form: *Intrusion Prevention Systems* (IPSs): Blockieren erkannte Attacken (z.B. adaptiv durch neue Firewallregeln)

- Ziel: Unternehmenskritische Daten erkennen und schützen
- Kategorisierung
 - Verwendete Daten: Daten, mit denen auf Endgeräten gearbeitet wird, z.B. Bestell- und Kundendaten, um eine Rechnung zu stellen
 - Übertragene Daten: Daten, die über das Netzwerk übertragen werden, z.B. eine Email mit einer Rechnung
 - Ruhende Daten: Daten, die gespeichert worden sind, z.B. eine archivierte (bezahlte) Rechnung auf einer Festplatte
- Aufzeichnung, wer wann und wie auf welche Daten zugreift → datenschutzrechtlich (teilweise) bedenklich
- Vermeidung von Datenabfluss (z.B. per USB-Stick oder Email)

Beispiel für ein DLP-System

How Data Loss Prevention Works



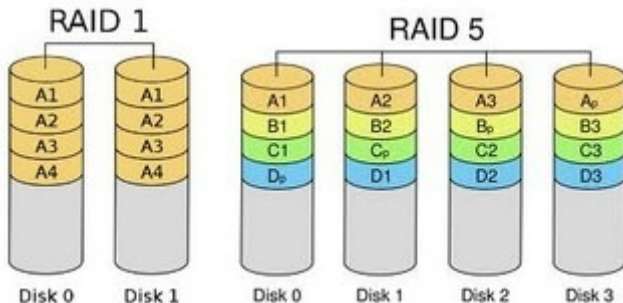
Quelle: Awareness Technologies: Data Loss Prevention. https://awarenesstechnologies.com/products_dlp.html (Zugriff am 25.3.2017), 2012.

- Grundvoraussetzung: Regelmäßige Überprüfung durch
 - Sicherheits-Checklisten für neue Systeme/Geräte
 - Penetration Testing (vgl. frühere Vorlesung)
 - Vulnerability Scanning (vgl. Erwähnung frühere Vorlesung)
 - Live-Überwachung (z.B. durch Einbrucherkennungssysteme)
 - Aufzeichnung (z.B. Log-Dateien, Zugriffsprotokolle)
- Orientierung an CIA-Schutzzielen
- Beispiele für Abwehrtechniken
 - Für Vertraulichkeit: Verschlüsselung, Zutrittskontrollen
 - Für Integrität: Signaturen, Zertifikate
 - Für Verfügbarkeit: **Redundanz**

- Redundante Serverinfrastruktur
 - Kritische Systeme wären „single point of failure“
 - Parallelsysteme betreiben
 - Teurer, aber ermöglicht im Fehlerfall Verfügbarkeit (Schutzziel)
- Redundante Hardware
 - Unterbrechungsfreie Stromversorgung
 - Zweites Netzteil, zweiter Prozessor u.ä.
- Redundante Netzwerkinfrastruktur
 - Router, Switches etc. redundant ausführen
 - Lastverteilung (engl. *load balancing*) zwischen mehreren Servern
- **Redundante Datenhaltung**
 - Daten doppelt (oder mehrfach) halten
 - Regelmäßige Datensicherungen durchführen
- Bei externem Hosting: Service Level Agreement (SLA) aushandeln

RAID (*Redundant Array of Independent Drives*)

- Sonderfall redundanter Datenhaltung: RAIDs
 - Daten redundant auf mehrere Festplatten verteilen
 - Ausfall einer Festplatte erlaubt (kurzfristig) Weiterbetrieb
 - Tausch der defekten Festplatte im Betrieb möglich (meist in Servern)
 - Verschiedene Level (z.B. 1: Spiegelung, 5: Verteilte Parität)



Quelle: Data Recovery YellowPages: RAID 1 Disadvantages. <http://www.datarecoveryunion.com/tag/raid-5/> (Zugriff am 25.3.2017), 2012.

- Arten von Datensicherungen
 - Gesamt (immer alle Daten speichern)
 - Differenziell (nur Unterschied zu letzter Sicherung speichern) → Wiederherstellung aus letzter Sicherung und Differenz möglich
 - Inkrementell (nur geänderte Daten speichern) → Wiederherstellung nur aus erster (Gesamt-)Sicherung und allen Differenzen möglich
- Zu berücksichtigende Aspekte
 - Welche Daten werden gesichert (Menge entscheidet über Kosten)?
 - Wie oft (z.B. täglich) werden die Daten gesichert?
 - Auf welches Medium (z.B. DVD) wird gesichert, wie lange hält es?
 - Welche Infrastruktur soll zur Sicherung verwendet werden?
 - Wo (geografisch) wird die Sicherung aufbewahrt?
 - Funktioniert die Wiederherstellung? → **Regelmäßig testen!**

- Engl. *business continuity management*
- Szenario: Katastrophales Ereignis, z.B.
 - Flugzeugeinschlag/Brand in Firmengebäude
 - Schwerer Sturmschaden in Datencenter (u.a. Daten verloren)
 - Tod der einzigen Person, die einen Schlüssel oder ein Passwort kennt
 - DoS-Attacke auf gesamte Serverinfrastruktur
- Macht Notfallplan (engl. *disaster recovery plan*) notwendig
 - Was wird im Fall X getan?
 - Wer ist wofür verantwortlich?
 - Wie kann der Betrieb (evtl. notdürftig) aufrecht erhalten werden?



Quelle: Advanced Computer & Data Communications: IT Network Disaster Recovery.
<http://acdcommunications.com/disaster-recovery.html> (Zugriff am 25.3.2017), 2016.

- Arten von Risiken (Auswahl)
 - Regulatorisch (z.B. neue Gesetze und Verordnungen)
 - Umweltbedingt (z.B. Sturm)
 - Operational (z.B. Stromausfall)
 - Technisch (z.B. Virenbefall)
 - Personell (z.B. Tod oder Krankheit eines Wissensträgers)
- Risikoabschätzung anhand von
 - Auftrittswahrscheinlichkeit
 - Dauer bis zur Reparatur/Wiederherstellung
 - Möglichem Schaden (nicht nur monetär)
- Erfordert entweder
 - Risikovermeidung (nicht immer möglich) oder
 - Risikoauslagerung (an Dritte) oder
 - **Risikoeindämmung (Abschwächung der Folgen)**

- Rechtebeschränkung
 - Benutzer haben minimale Zugriffsrechte (z.B. auf Dateien)
 - Zugriff bei Kompromittierung eingeschränkt
 - Beispiel: Zugriff auf Backupsystem nur durch dedizierte Mitarbeiter
 - Erfordert Erfassung und Einschränkung von Rechten
 - Erfordert Dokumentation und regelmäßige Aktualisierung
- Änderungsmanagement
 - Alle sicherheitsrelevanten Änderungen dokumentieren
 - Vermeidet (versehentliche) Aufhebung oder Rückgängigmachung bestehender Sicherheitsmechanismen
 - Erlaubt Wiederherstellung früherer Zustände
 - Beispiel: Neues Gerät gekauft oder bestehendes Gerät umfunktioniert
 - Erfordert Dokumentation → zeit- und ressourcenaufwändig
 - Zusätzliches Risiko: Dokumentation muss gespeichert werden
- Vorfallsmanagement (wie genau bei Vorfällen reagieren?)

- Sicherheitsrichtlinien
 - Beantworten Frage: Wie werden Assets geschützt?
 - Dokumentierte Beschreibung mit Risikoeinschätzung
 - Definieren Vertrauensmodell (wem wird inwieweit vertraut?)
 - Definieren Benutzer-/Mitarbeiterverhalten inkl. Konsequenzen
 - Beispiel: **Passwortrichtlinien** (Vorgaben für minimale Länge, Komplexität, maximales Alter; Beschränkung der Login-Versuche)
 - Bedürfen regelmäßiger Evaluierung
- Mitarbeiterschulungen
 - Regelmäßiges Training der Mitarbeiter
 - Hauptziel: Mitarbeiter halten Sicherheitsrichtlinie ein
 - Nebenziel: Mitarbeitern ist die Existenz von Richtlinien bewusst
 - Beispiel: Woran erkennt man verdächtige Emailanhänge?
 - Weiteres Beispiel: Wen kontaktieren bei Ransomware?
 - Fundamentaleres Beispiel: Wo können Richtlinien nachgelesen werden?

- Ziele
 - Hergang eines Angriffes (z.B. Datenmanipulation) rekonstruieren
 - Spuren sichern → erlaubt Korrektur und erleichtert Strafverfolgung
 - Retten, was noch zu retten ist (z.B. Datenfragmente)
- Beispiel: Spurensicherung von angegriffenem Rechner
 - Nicht herunterfahren (Daten würden verloren gehen)
 - Arbeitsspeicher sichern (nicht trivial!)
 - Offene Netzwerkverbindungen aufzeichnen
 - Laufende Prozesse sichern
 - Benötigt Spezialsoftware
- Spuren werden zu Beweiskette zusammengesetzt
- Benötigt tiefgehendes (System-)Wissen
- Antiforensik: Forensik zu erschweren oder unmöglich machen

Fragen?