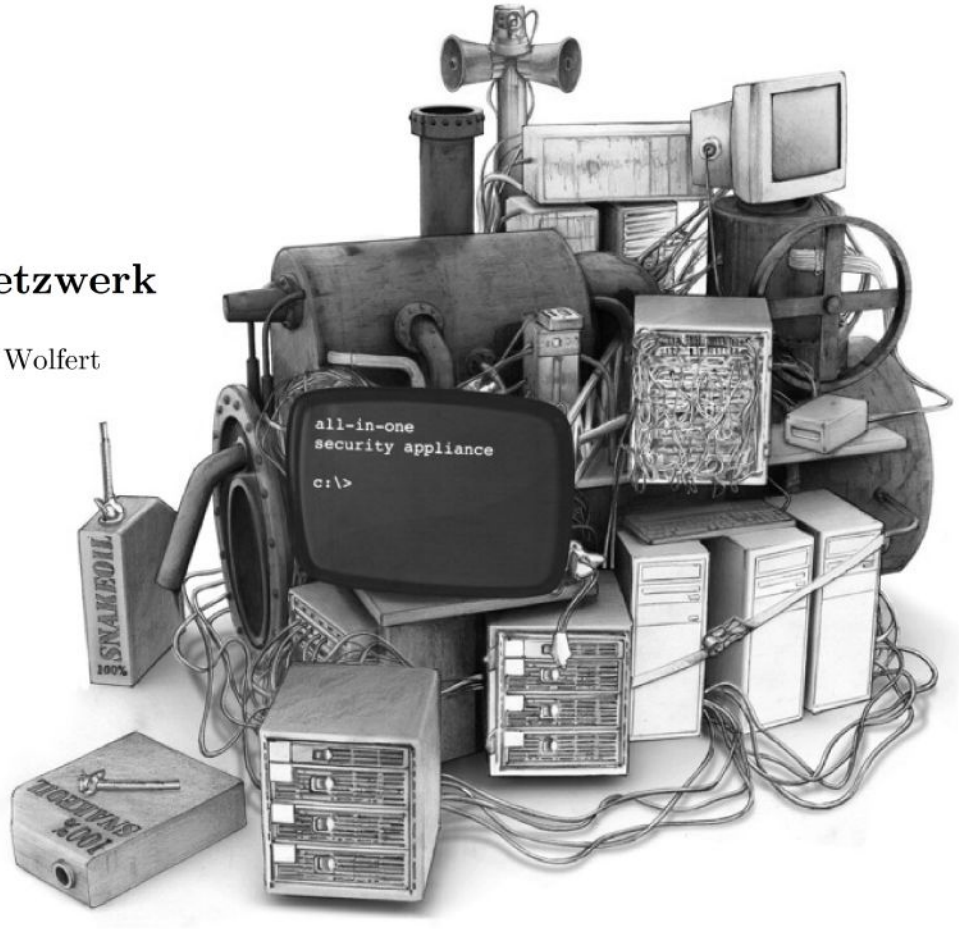
Boom der digitalen Spionage

Zielgerichtete Angriffe auf das Unternehmensnetzwerk

Regionalgruppe München GI&GChACM | 06. Oktober 2014 | Christoph Wolfert



"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" - Bruce Schneier

SCHUTZWERK

Unabhängige Prüfung – ganzheitliche Optimierung

SCHUTZWERK ist Ihr Partner für die unabhängige Prüfung und ganzheitliche Optimierung aller Aspekte der Informations- und IT-Sicherheit in Ihrem Unternehmen.

1 Einleitung

2 Vorgehensweise der Angreifer mit Demonstrationen

3 Maßnahmen

4 Fazit

1 Einleitung

2 Vorgehensweise der Angreifer mit Demonstrationen

3 Maßnahmen

4 Fazit

▶ Begriffsdefinition: Zielgerichteter Angriff

> Im Englischen auch „Targeted Attacks“ genannt

> Grundsätzlich verfolgt jeder Angriff ein bestimmtes Ziel

> Die Unterschiede zu einem „gestreuten“ Angriff liegen im Wesentlichen in der Vorgehensweise sowie Auswahl der Zielsysteme

▶ Abgrenzung

„Gestreute“ Angriffe	Zielgerichtete Angriffe
- automatisiert - großer Bereich an Zielsystemen - hohe Abdeckung Motivation: - Erlangung „beliebiger“ wertvoller Daten (z.B. Kreditkartennummern, Adressbestände mit E-Mail-Adressen etc.)	- weitestgehend manuell - dedizierte Zielsysteme - Sammlung von Informationen im Vorfeld über das Zielsystem - Spezifische Anpassung von z.B. Schadcode für das Zielsystem Motivation: - Erlangung besonders wertvoller Informationen (z.B. Firmen-Know-how) - Abhören v. Kommunikation (z.B. Strategiegespräche) - Manipulation von IT-Systemen (z.B. Kraftwerks-steuerung)

- **Zielgerichtete Angriffe auf IT-Infrastrukturen von Behörden und Firmen haben in den letzten Monaten stark zugenommen**
  - > Diebstahl von sensiblen Informationen
  - > Störung des produktiven Betriebs
- **Die zielgerichteten Angriffe gehen häufig aus von**
  - > ausländischen Nachrichtendiensten[1],
  - > Militäreinheiten[2],
  - > Hackergruppen (mit Regierungsauftrag[3]) oder
  - > hochorganisierten Internet-Kriminellen
- **Über das Thema der zielgerichteten „Cyber-“ und „Hackerangriffe“ wird in den Medien vermehrt berichtet**

[1] http://www.heise.de/newsticker/meldung/Berichte-Hacker-griffen-Firmen-und-Behoerden-an-1809564.html
[2] http://www.heise.de/security/meldung/Bericht-Chinesische-Hacker-mit-Regierungsauftrag-1805861.html
[3] http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

- **Beispiele aus bekannten Online-Medien für zielgerichtete Angriffe aus dem Jahr 2014**
  - SPIEGEL ONLINE [1]
    - 21.09.2014: Staatsanwaltschaft ermittelt nach mutmaßlichem Cyberangriff auf deutsche Firma
    - 17.07.2014: Hackerangriff bremst Geschäft von Ebay
    - 19.05.2014: USA klagen erstmals Chinesen wegen Cyberspionage an
    - etc.
  - heise [2]
    - 19.09.2014: Hackerangriff auf Home Depot: 56 Millionen Kreditkarten betroffen
    - 28.08.2014: FBI untersucht Hackerangriff auf Großbanken
    - 19.08.2014: Hacker erbeuten Daten von 4,5 Millionen Patienten in den USA
    - 19.08.2014: Mehrere erfolgreiche Angriffe auf US-Atombehörde NRC
    - 24.07.2014: Hacker erbeutet 20.000 E-Mail-Adressen bei der Europäischen Zentralbank
    - etc.
- **Suchbegriffe: Hackerangriff, Cyberkrieg, Cyberangriff etc.**

[1] www.spiegel.de / [2] www.heise.de

- **Häufigste Motivationen zur Durchführung eines Zielgerichteten Angriffs auf Unternehmen:**
  - Industrie-/Wirtschaftsspionage
  - Schattenwirtschaft
  - Schädigung von Konkurrenzunternehmen
  - etc.

▶ Zahlen und Fakten am Beispiel: Industrie-/Wirtschaftsspionage[1]

- > Jedes zweite Unternehmen hatte in den vergangenen beiden Jahren einen Spionageangriff oder Verdachtsfall zu beklagen (Anstieg von 5.5% im Vergleich zu 2012)
- > Der jährliche finanzielle Schaden durch Industriespionage beläuft sich in Deutschland auf 11,8 Milliarden Euro
- > 77% der Unternehmen in Deutschland hatten einen finanziellen und mehr als ein drittel aller Unternehmen einen materiellen Schaden zu verzeichnen
- > Nach wie vor steht der Mittelstand verstärkt im Fokus der Angreifer
- > etc.

[1] Studie: Corporate Trust - Industriespionage 2014
(siehe https://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf auf Seite 8)

- **Das BSI startete Anfang November 2012, in Zusammenarbeit mit dem Bundesverband Informationswirtschaft und der BITCOM, die Initiative „Allianz für Cybersicherheit“ [1]**
  - > Ziel ist es
    - aktuelle und valide Informationen flächendeckend bereitzustellen,
    - eine umfangreiche Wissensbasis aufzubauen sowie
    - den Informations- und Erfahrungsaustausch zu unterstützen

[1] Allianz für Cybersicherheit (siehe https://www.allianz-fuer-cybersicherheit.de)

- **11/2012: Innenministerium plant IT-Sicherheitsgesetz[1]**
  - > Internetprovider sollen Kunden Auskunft über Schadsoftware sowie Mittel zur Störbeseitigung bereitstellen
  - > BSI soll zukünftig Hard- und Softwarekomponenten untersuchen und die Ergebnisse veröffentlichen
- **04/2013: Wirtschaft wettert gegen geplantes IT-Sicherheitsgesetz[2]**
  - > IT-Branchenverband Bitkom bezweifelt Handlungsbedarf
  - > „Allianz für Cybersicherheit“ ist besser geeignet
- **11/2013: Friedrich will IT-Sicherheitsgesetz durchsetzen[3]**
  - > Datenverkehr in Europa soll ausschließlich über europäische Netze geleitet werden
  - > Strengere IT-Sicherheitsstandards

[1] http://www.heise.de/security/meldung/Innenministerium-plant-IT-Sicherheitsgesetz-1746002.html
[2] http://www.heise.de/security/meldung/Wirtschaft-wettert-gegen-geplantes-IT-Sicherheitsgesetz-1833835.html
[3] http://www.handelsblatt.com/politik/deutschland/koalitionsverhandlungen-friedrich-will-it-sicherheitsgesetz-durchsetzen/9022878.html

▶ 08/2014: Innenminister veröffentlicht Entwurf für IT-Sicherheitsgesetz[1]

> Gesetzliche Meldepflicht von IT-Sicherheitsvorfällen und die Einhaltung von „IT-Mindeststandards“

> Höhere IT-Sicherheitsstandards der Telekommunikationsanbieter (Provider)

> Verbindliche Vorgaben für das Schutzniveau der IT-Systeme des Bundes durch das BSI

> Stärkung der Rolle des BSI durch klarere „Warnbefugnisse“ und durch die Etablierung des BSI als internationale Zentralstelle für IT-Sicherheit.

> Ausweitung der Rolle des BKA auf dem Gebiet der Strafverfolgung

[1] http://www.heise.de/security/meldung/Innenminister-veroeffentlicht-Entwurf-fuer-IT-Sicherheitsgesetz-2294637.html

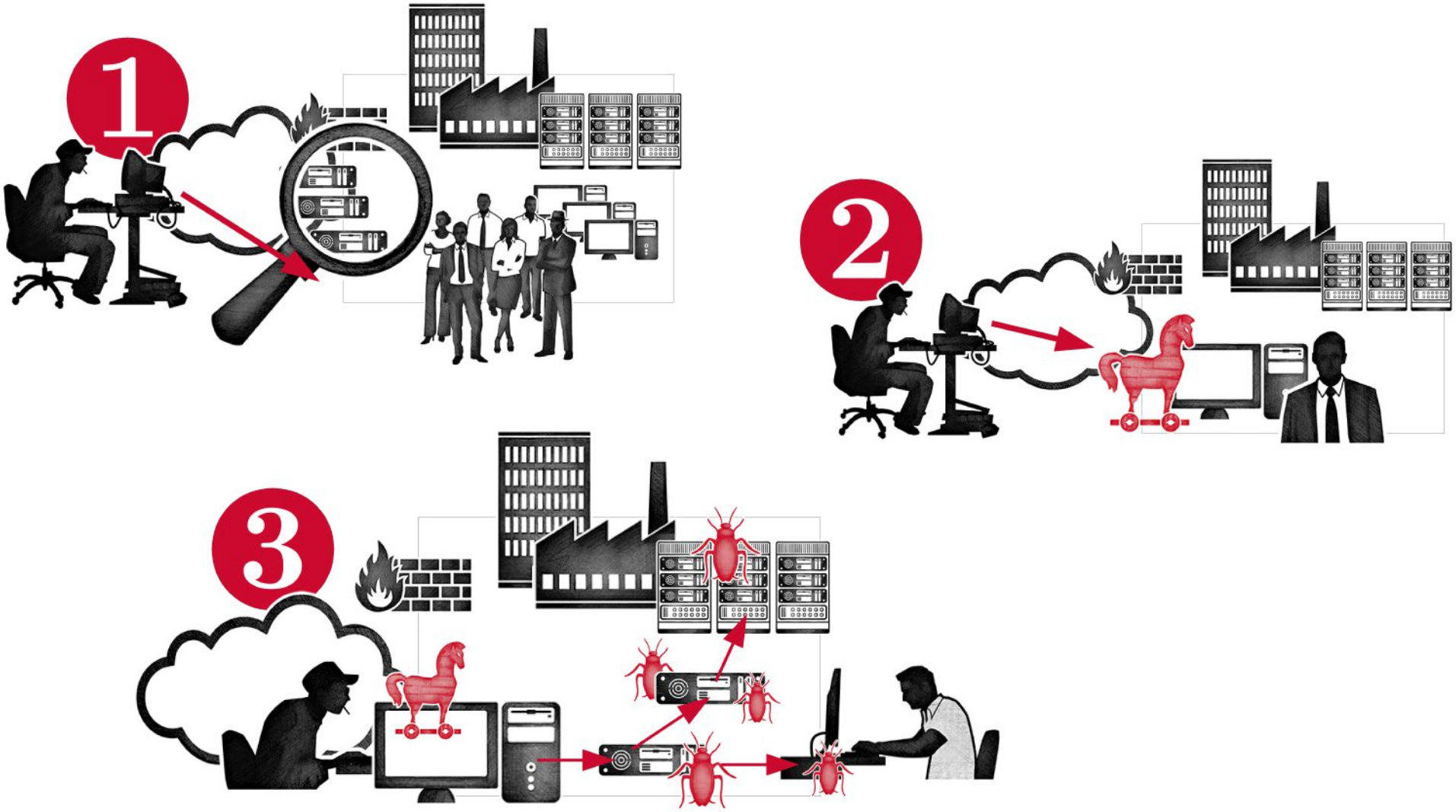
1 Einleitung

2 Vorgehensweise der Angreifer mit Demonstrationen

3 Maßnahmen

4 Fazit

Die drei verschiedenen Phasen eines zielgerichteten Angriffs



Phase 1: Vorbereitung

- **Sammeln von Informationen (Information Gathering)**
  - Öffentlich verfügbare Informationsquellen
    - Internet
      - Websites des Unternehmens
      - (Personen) Suchmaschine
      - Schlüsselserver
      - Social Media
      - Online-Footprinting
      - Auswertung von Metadaten
    - Messen/Ausstellungen
    - Observation von Firmengebäuden, Personen etc.
  - Tools können die Arbeit erleichtern, wie z.B.:
    - theHarvester [1]
    - Metagoofil [1]
    - Maltego [2]

[1] http://www.edge-security.com/portfolio.php
[2] http://www.paterva.com/web6/products/maltego.php

Phase 1: Vorbereitung

- **Ausnutzen von menschlichen Eigenschaften/Verhaltensweisen zur Informationsgewinnung (Social Engineering)**

  > Abgrenzung

„menschlich / persönlich“	„technisch“
- Ausgeben als Mitarbeiter oder autorisierter Benutzer (Impersonating) - Anruf beim technischen Support - Über die Schulter schauen (Shoulder Surfing) - An Mitarbeiter anhängen (Tailgating)	- E-Mail Anhänge (E-Mail Attachments) - Gefälschte Webseiten (Fake Websites) - Phishing Angriffe via E-Mail - Scam Angriffe via E-Mail

  > Tools

  - Social Engineering Toolkit (SET) [1]

[1] https://www.trustedsec.com/downloads/social-engineer-toolkit/

Phase 2: Initialer Angriff

- **Eindringen in das Firmennetzwerk (Live Demonstration)**

  > Einbettung von schadhaftem Code in einer vertrauenswürdig aussehenden PDF-Datei und Versand per E-Mail an das Opfer

  > Bereitstellung eines vertrauenswürdig aussehenden Links (z.B. via E-Mail), der das Opfer im Hintergrund auf die Webseite des Angreifers leitet

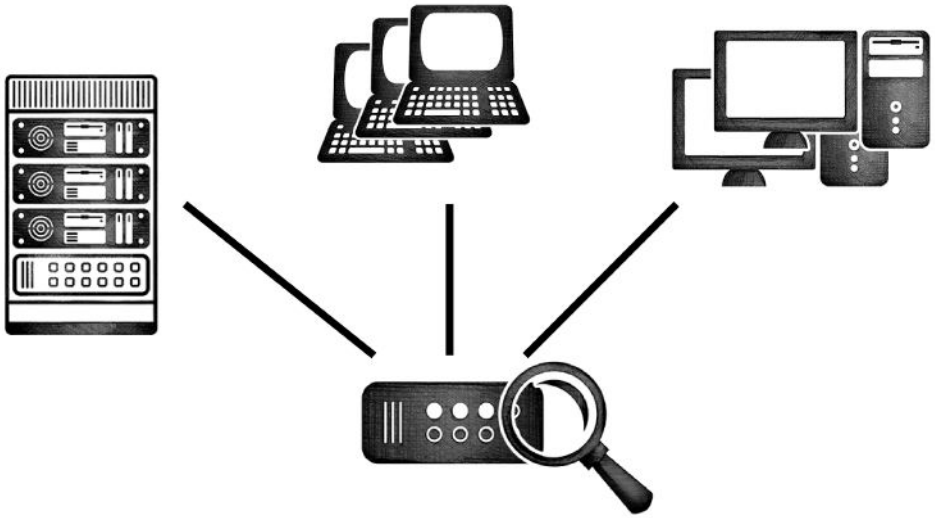
  > Folgende Herausforderungen stellen sich dabei dem Angreifer:

  - Umgehung des Virenscanners auf E-Mail-Server, Zielsystem etc.
  - Finden von geöffneten Diensten vom Unternehmensnetzwerk ins Internet
  - Identifikation der installierten Softwareversionsstände auf dem Zielsystem

3

Phase 3: Weiterführende Angriffe innerhalb des Firmennetzwerks

- **Überblick verschaffen**
  - > Passives Mitlesen des Datenverkehrs
    - Datenaufzeichnung (z.B. wireshark, tcpdump)
  - > Wo befinde ich mich als Angreifer?
    - Adressbereich (IP-Adresse)
    - Namensraum (DNS)
  - > Was befindet sich um mich herum?
    - Aktive Systeme (z.B. nmap, ping)
    - Verfügbare Dateifreigaben (z.B. smb tree)
    - etc.



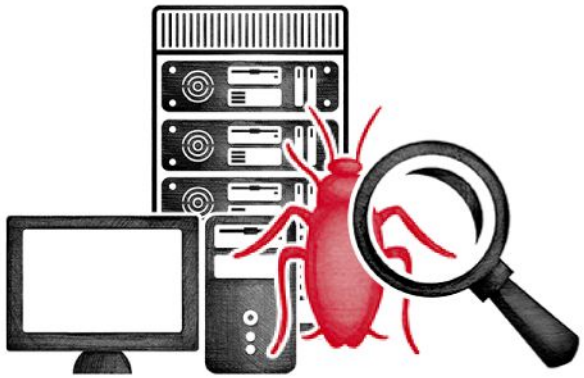
Phase 3: Weiterführende Angriffe innerhalb des Firmennetzwerks

3

▶ Identifikation interessanter „Assets“

> Interessante „Assets“ sind z.B.
  - Zentrale Systeme (DC, File Server, DB, Telefonanlage etc.) die Schwachstellen aufweisen oder
  - Systeme deren Schwachstellen ohne großen Aufwand auszunutzen sind (z.B. MS08-067)

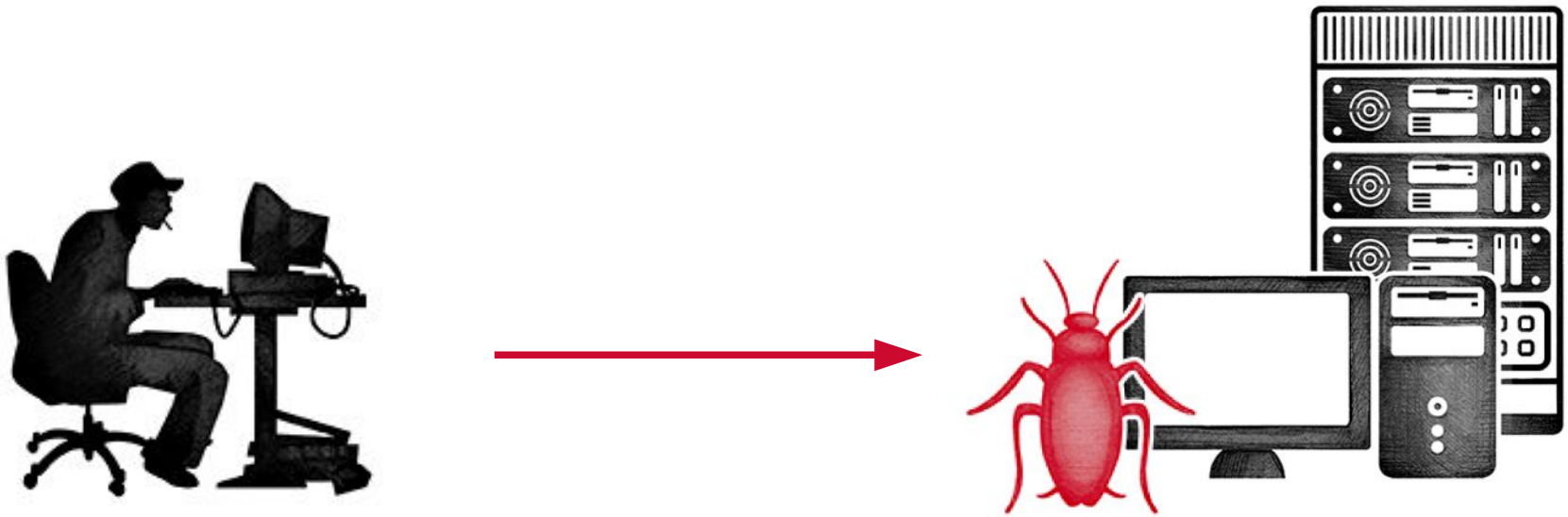
> Interessante „Assets“ lassen sich beispielsweise über folgende Methoden identifizieren:
  - Systeme und deren angebotene Dienste lassen sich über einen Portscanner (z.B. NMAP) ermitteln
  - Sogenannte Schwachstellenscanner (z.B. Nessus oder Greenbone) unterstützen bei der Suche nach Sicherheitsmängeln, die sich für einen Angriff ausnutzen lassen



Phase 3: Weiterführende Angriffe innerhalb des Firmennetzwerks

3

- **Angriff von „schwachen“ Zielen**
  - > Ausnutzen der sogenannten Conficker-Schwachstelle (MS08-067) auf einem Windows XP System
  - > Angriff von sog. Administrative Shares auf einem Windows 7 System
  - > etc.



Phase 3: Weiterführende Angriffe innerhalb des Firmennetzwerks

- **Zugriff auf wichtige Informationen (Live Demonstration)**
  - > Auslesen sowie entschlüsseln der Passwortdatenbank eines Windows XP Systems
  - > Zugriff auf Passwörter in einem Windows 7 System ohne Entschlüsselung der Passwortdatenbank

Phase 3: Weiterführende Angriffe innerhalb des Firmennetzwerks

- **Ausweitung des Angriffs auf weitere Systeme**
  - > Verwendung von Standardbenutzern um Zugriff auf Systeme zu erlangen, deren Benutzer nicht über die zentrale Domäne verwaltet werden
    - Datenbanken
    - Webserver
    - etc.
  - > Die ermittelten Zugangsdaten können dazu verwendet werden um beispielsweise
    - auf Gruppenlaufwerke oder
    - weitere Dateifreigaben zuzugreifen
  - > Übernahme der gesamten Windows Domäne durch die Erstellung eines eigenen Domänenadministrators
    - Anmelden an beliebigen Systemen, welche über die zentrale Domäne verwaltet werden
    - Zugriff auf sensitive Informationen möglich

1 Einleitung

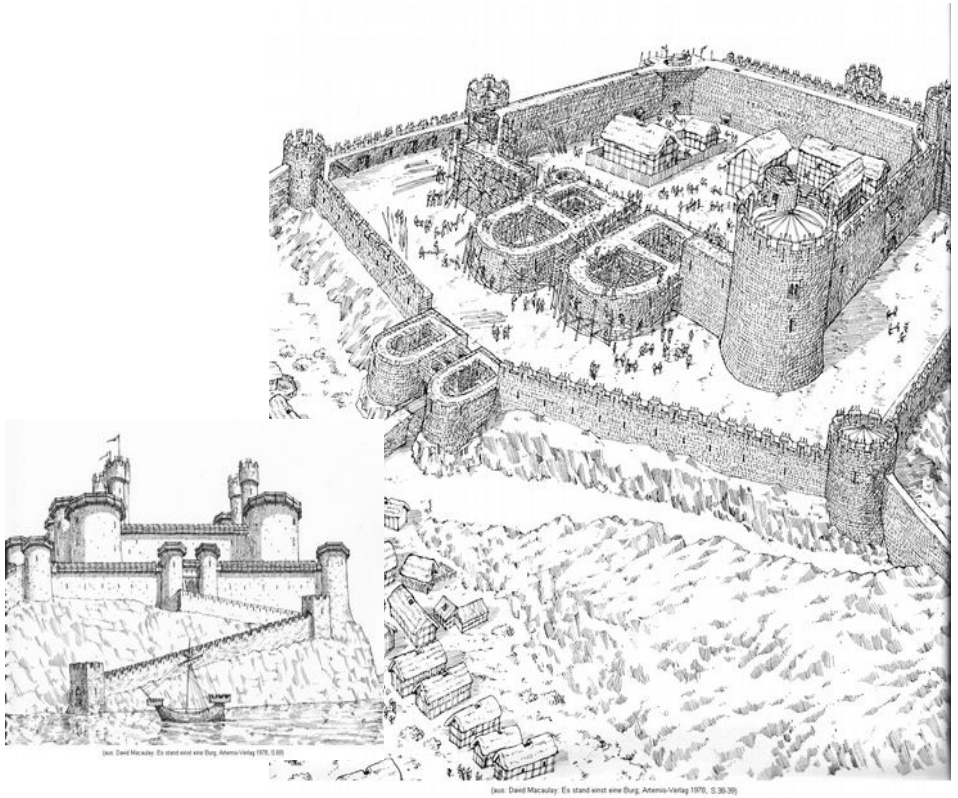
2 Vorgehensweise der Angreifer mit Demonstrationen

3 Maßnahmen

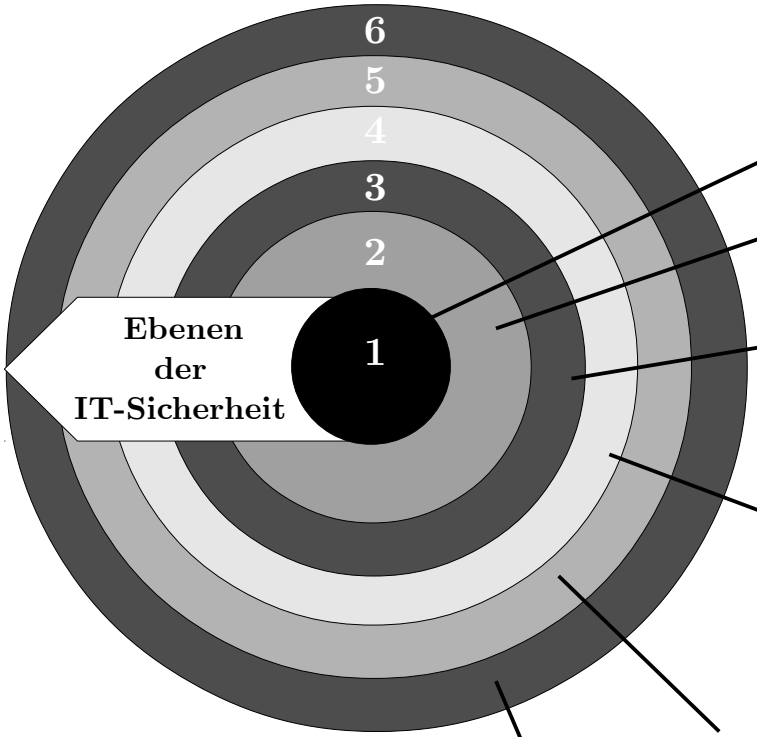
4 Fazit

Nachhaltige Sicherheit vor zielgerichteten Angriffen bedingt...

- ...eine Mehrstufigkeit der Sicherheitskonzepte...
- ...ausgehend von den Werten (Daten) und kritischen Geschäftsprozessen des Unternehmens...
- ...unter Einbeziehung des Menschen...
- ...in Verbindung mit Prozessen
- **Fundament bildet der Informations-sicherheitsmanagement-Prozess (auf Basis IT-Grundschutz bzw. ISO/IEC 27001)**



Mehrstufigkeit der Sicherheitskonzepte (1)



Daten / kritische Geschäftsprozesse des Unternehmens

Sicher konzipierte und betriebene IT-Systeme (Härtung, Patchmm. etc.)

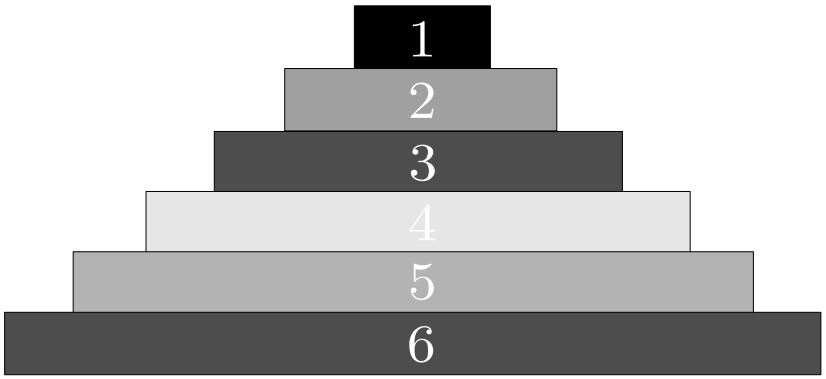
Technische Sicherheitsvorkehrungen (Virenschutz, Firewall, Backup, RZ-Sicherheit etc.)

Organisatorische Maßnahmen in der IT (Dokumentationsrichtlinien, Notfallplanung, Incident Management etc.)

Übergreifende, organisatorische Maßnahmen (Arbeitsanweisungen für Mitarbeiter, Schulungen, Datenschutz etc.)

Informationssicherheitsmanagement / Compliance / Revision

Mehrstufigkeit der Sicherheitskonzepte (2)



1 = **Zu schützender Wert** (Anforderung: Vertraulichkeit, Integrität und Verfügbarkeit – Daten / Geschäftsprozesse als „Kern“ der Informations- & IT-Sicherheit)

2 + 3 = **Technische und konzeptionelle Ebenen**

4 + 5 = **Menschliche (personelle) und konzeptionelle Ebenen** („tragende Rolle“ der menschlichen Sicherheitsaspekte)

6 = **Steuerungs- und Prüfungsebene** (Informationssicherheitsmanagement als prozessbasiertes „Fundament“ der Informations- und IT-Sicherheit)

Mehrstufigkeit der Sicherheitskonzepte in der Praxis, am Beispiel der PCs & IT-Benutzer:

> Geschäftsleitung definiert Sicherheitspolitik (IT-Sicherheitsleitlinie in Verbindung mit Benutzerrichtlinien)

> Benutzer sind im Umgang mit IT-Systemen und Daten geschult und sensibilisiert

> IT-Systeme der Benutzer sind gehärtet und vor Missbrauch geschützt (keine Adminrechte, Virenscanner, Verschlüsselung etc.)

> Systeme des Benutzers sind in das Patchmanagement integriert

> Zugriffsrechte der Benutzer sind im Rollen- & Rechtekonzept klar definiert

> Zugriffsmöglichkeit im Netzwerk und auf Systeme sind technisch eingeschränkt (Segmentierung, technische Forchierung des Rollen- & Rechtekonzepts)

1 Einleitung

2 Vorgehensweise der Angreifer mit Demonstrationen

3 Maßnahmen

4 Fazit

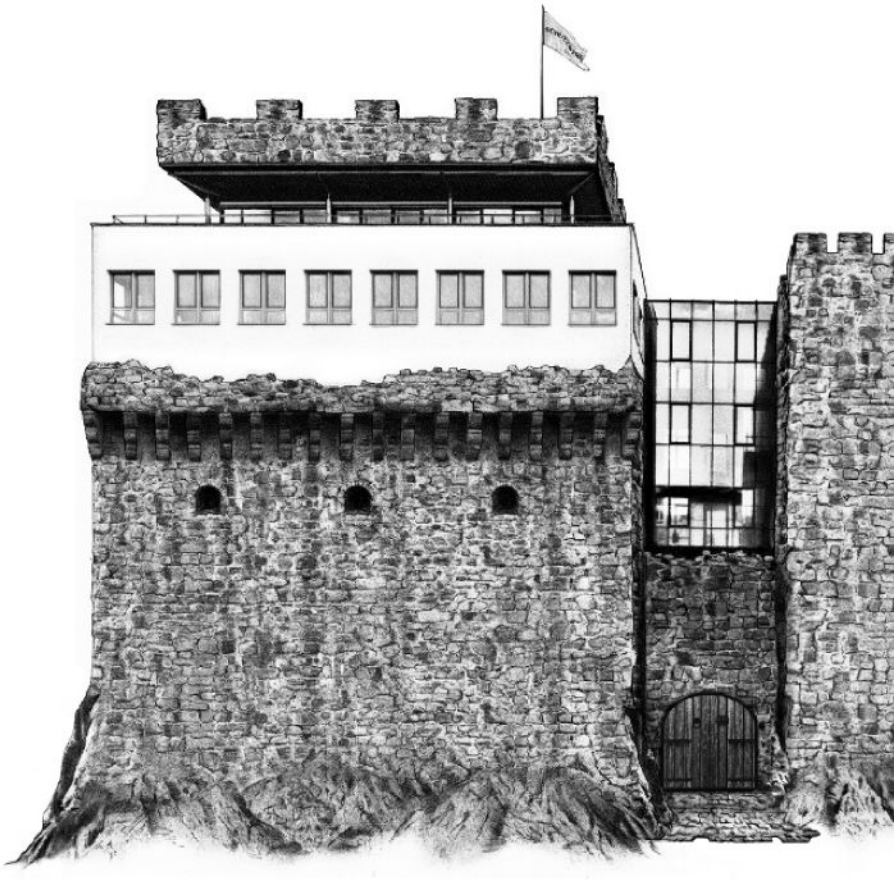
- Die Bedrohung der Unternehmen durch digitale Spionage und Internet-Kriminalität steigt
- Ein häufiges Ziel der Angreifer sind Client-PC, als „Brückenkopf“ ins interne Netzwerk
- Durch immer ausgeklügeltere Methoden (z.B. Trojanische Pferde in Kombination mit Social Engineering) kann ein Erfolg der Angriffe nie vollständig ausgeschlossen werden
- Fällt die erste „Verteidigungslinie“, ist die Qualität weiterer Sicherheitsmaßnahmen von entscheidender Bedeutung
- Nachhaltige Informations- und IT-Sicherheit im Unternehmensnetzwerk kann daher nur durch
  - > **eine Mehrstufigkeit der Sicherheitskonzepte**
  - > **in Verbindung mit entsprechenden Prozessen (Organisation und Mensch)**

  gewährleistet werden

SCHUTZWERK

SCHUTZWERK GmbH
Pfarrer-Weiß-Weg 12
89077 Ulm

Phone +49 731 977 191 0
Fax +49 731 977 191 99

www.schutzwerk.com
info@schutzwerk.com

Für Fragen stehen wir
Ihnen gerne zur Verfügung