Erkennung von und Umgang mit mehrstufigen komplexen Angriffsszenarien

Basisschutz erweitern!

Effiziente Lösungen bei der Abwehr von Angriffen auf das Netzwerk

Dr. Roland Kaltefleiter rk@NetUSE.de
NetUSE AG https://www.netuse.de/

11.11.2015 DiWiSH Forum IT-Sicherheit

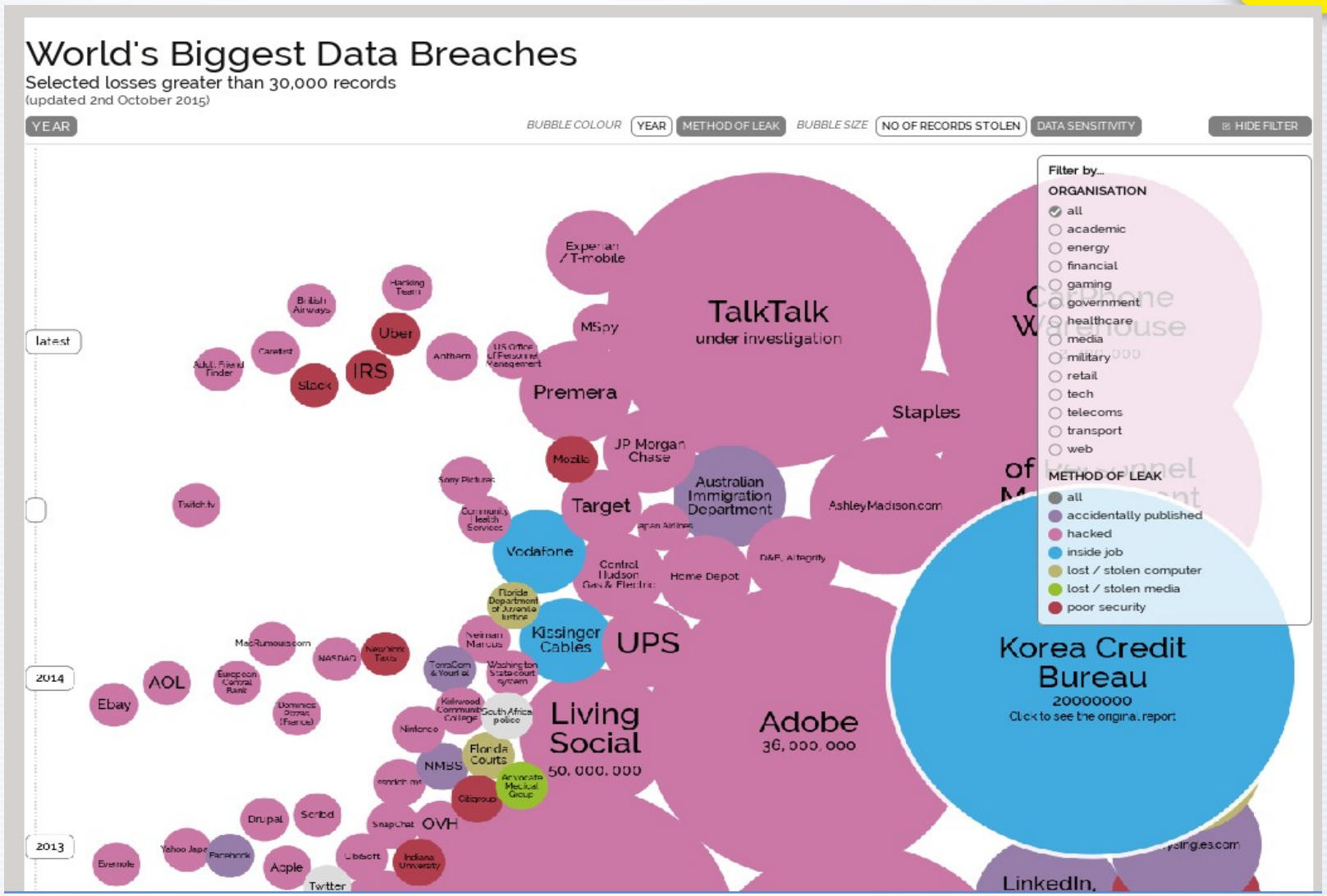
Über die NetUSE AG

- Seit 1992 am Markt
  - Seit 1994 IT-Security
  - 2 eigene RZs in Kiel
  - Zugriff auf RZ mit ISO 27001: 2013 Zertifizierung
- 70 Mitarbeiter
- 2014/2015: ca. 12,5 Mio € Umsatz

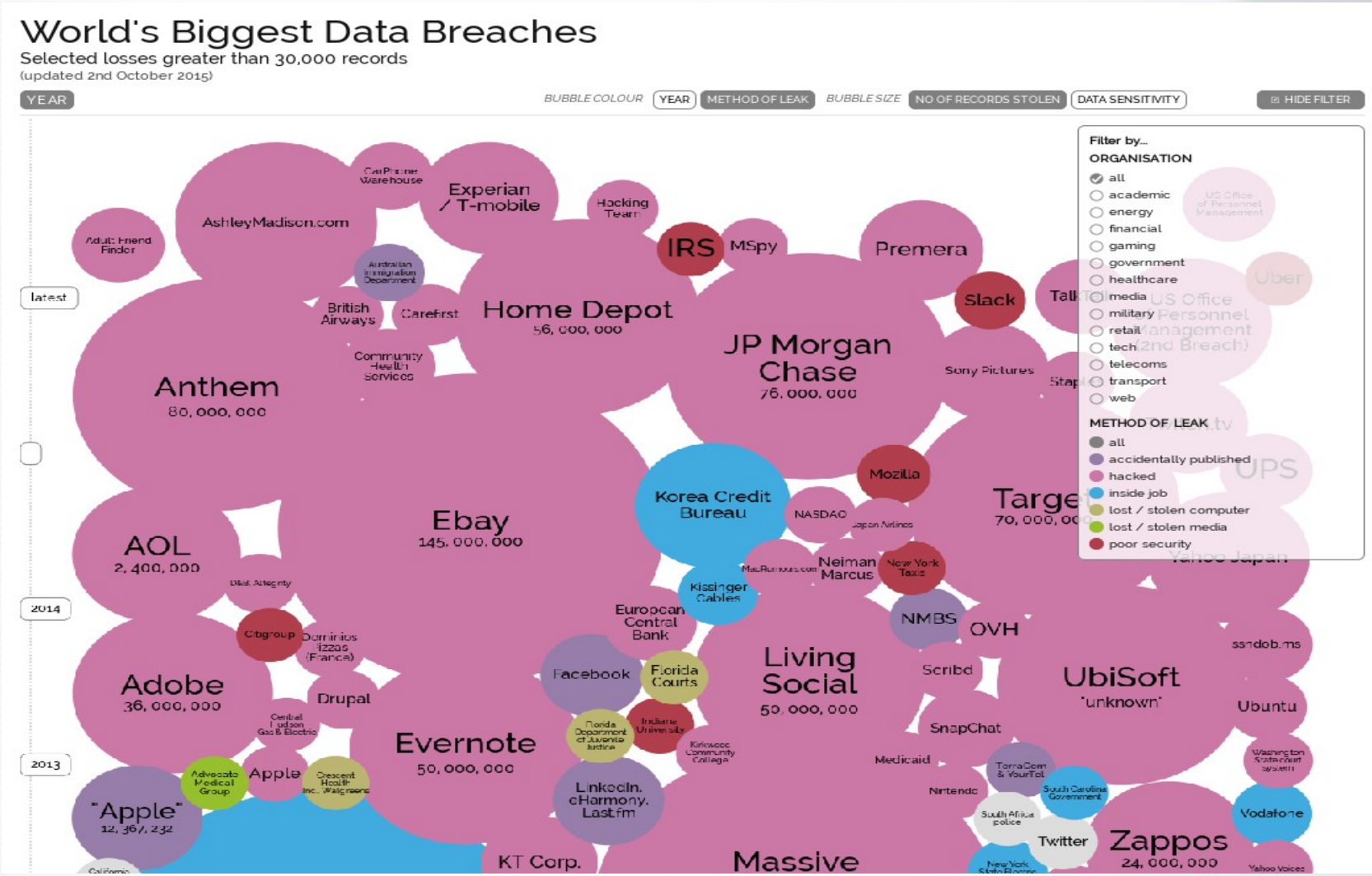
https://www.netuse.de/

Agenda

- Einführung
- Angriffsszenarien
- Angriffserkennung
- Management IT-Security
- SOC



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Dann war da noch ….

- „Der Bundestagshack“

  In der Kurzfassung ….

  - „Klassischer Angriff“ mit
    - Spear-Phishing-Mail und folgend Drive-By-Download von Malware

Noch ein paar Zahlen aus einem Test der NetUSE AG

- 1. Frage: Wer von ihnen hat einen Linux-Server, der mit Login/Passwort erreichbar ist, im Internet stehen?
- 2. Frage: Lesen sie dort auch mal die Systemlogs?
- Grundrauschen sind laufende Passwordscans aus Bot-Netzen ca 1 Versuch / Sekunde
  => 90.000 am Tag
  => 32 Mio im Jahr

  Das sind Bots, die das Netz kartographieren!

Angriffsszenarien: Komplex - mehrstufig

- Massenangriffe im Privat-Bereich:
  - Sie haben E-Mail von ihrer Bank …
  - DHL Mail mit „zip“
- Gezielte Angriffe:
  - Zugriff auf das Netzwerk bekommen
    => Erfordert oft mehr als eine Infektion

Beispiel

- Recherche liefert die Info, „SIE“ arbeiten mit einem Coach X (Freiberufler) zusammen.
- Wer betreute die Webseite: Agentur Y in Klein Dorf
- Geziele Malware auf die (kleine) Agentur
  - Ziel: PCs verseuchen, Keylogger installieren
  - Zugangsdaten zu Webseite des Coaches abgreifen
- Webseite des Coaches „vorbereiten“ für gezielten Malware-Download

Beispiel: Fortsetzung

- „Phishing“-Mail in Form eines Web-Newsletters an Führungspersonen „Ihres“ Unternehmens vom Server des Coaches
- „Bitte hier Klicken für mehr Infos.....“ und schon kommt die Malware
  - AV wird scheitern, weil die Malware „unique“ ist
  - Reputation wird scheitern, weil IP im Prinzip gut
  - Malware war nur kurz auf dem Server

Quelle: http://www.heise.de/security/meldung/Patchday-Microsoft-macht-Windows-und-seine-Webbrowser-sicherer-2916526.html

Weitere Bausteine

- USB – Smartphones/Tablets
- WLAN (an Flughäfen, Hotels)
- Notebooks ohne Festplatten Verschlüsselung / BIOS-Schutz (wegen Boot)
- Apps.....
- Bluetooth

Angriffserkennung

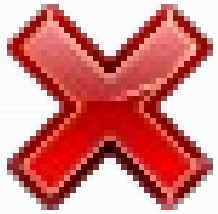
- Wer hat im Einsatz:
  - Gateway-Firewall (auch Next Generation)
  - Anti-Virus und Personal-Firewall
  - IDS – IPS – DLP
  - Network Access Control - NAC
  - VPN – mit 2FA
  - Threadanalysis (Sandboxing)
  - Mobile-Security (mehr als nur Wipen)
  - Database-Security
  - Data@Rest-Encryption
  - SIEM

Angriffserkennung

- Wer hat im Einsatz, übliche Verteilung:
  - Gateway-Firewall (auch Next Generation)
  - Anti-Virus und Personal-Firewall
  - IDS – IPS – DLP ?
  - Network Access Control - NAC ?
  - VPN – mit 2FA?
  - Threadanalysis (Sandboxing)?
  - Mobile-Security
  - Data@Rest-Encryption
  - SIEM

Angriffserkennung

- Vorarbeiten erforderlich
- Daten (Logs, Netzwerkdaten etc.) erheben und zentral sammeln
  - Jedes Gerät und jede Anwendung liefern Daten
- Ist-Zustand ermitteln → Soll-Zustand festlegen



- Zu schnelle Änderungen => nicht manuell machbar

Angriffserkennung

- Lösung: SIEM

- Was macht ein SIEM?
  - Sammelt möglichst viele Daten und korreliert diese wenn möglich in Echtzeit

    => Man sieht den Wald trotz vieler Bäume!

- Aber auch ein SIEM muss betrieben werden!

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (July 2015)

Erkenntnis

- Grundregel:
  - Der Security-Breach wird kommen, bei jedem!
  - Das ist wie im Straßenverkehr, sie können immer in einen Unfall verwickelt sein!
- Frage: Sind Sie auf solche Incidents vorbereitet?

Management IT-Security

- Awareness schaffen
  - Offene Informationskultur
  - „Es kann jeden Mitarbeiter erwischen!“
  - „Es gibt keine dummen Fragen!“
- Security-Policy
  - Muss verständlich sein!
    - Maximal 50 Seiten!
  - Jeder Mitarbeiter muss diese kennen und leben!

Management IT-Security

- Updates sofort einspielen!
  - Auf allen Geräten!
- Trennung der IT in Zonen
  - „internes Firewalling“
- Haben sie schon mal einen Angriff simuliert und den Umgang damit geübt?

Management IT-Security

- Bei einem KMU ist der monatliche Aufwand für die Security-Infrastruktur weniger als eine volle Stelle.
- Das Know-How muss immer aktuell sein!
- Eine Reaktion muss sofort erfolgen.
- Personal muss verfügbar sein (mind. 3 Personen, ggf. mehr)
- Hat das Personal praktische Erfahrung?

=> **Ist das wirtschaftlich?**

SOC – Security Operations Center

Typische Dienstleistungen eines SOC:

- Proaktive Analyse und Verwaltung der Systeme und Technologien der EDV-Sicherheit
- Security Device Management
- Reporting
- Security Alert
- DDoS Schadensbegrenzung
- Security Assessment
- Technische Hilfe

Bitte fragen sie uns (NetUSE) zu diesen Themen!

Vielen Dank für ihre Aufmerksamkeit!

Fragen?