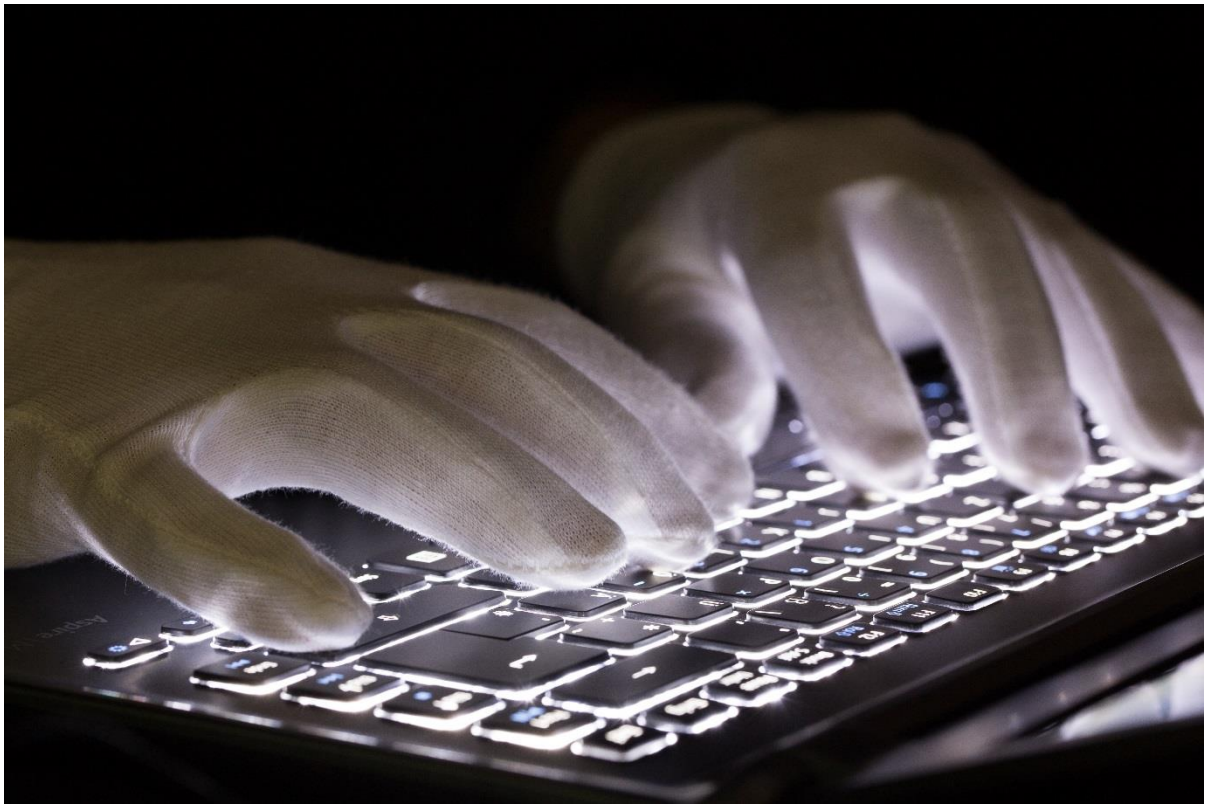
Cybercrime

Aktuelle Lage und Phänomene / Februar 2017



KOK Olaf Borries, LKA 245 Cybercrime

ZAC Berlin – Zentrale Ansprechstelle Cybercrime

Cybercrime

Aktuelle Lage und Phänomene / Februar 2017

Laut Ankündigung des Vortrags:

Herausforderungen der Digitalisierung und IT-Sicherheit
Gesundheitsdaten und deren (Untergrund-) Wert
Aktuelle Phänomene und Angriffsvektoren
Ganzheitliches Sicherheitskonzept
Polizeiarbeit im Falle eines Cyberangriffs

KOK Olaf Borries, LKA 245 Cybercrime
ZAC Berlin – Zentrale Ansprechstelle Cybercrime

Übersicht

1. Vorstellung der Dienststelle
2. Wer wird angegriffen?
3. Wer greift an?
4. Was sind die Ziele von Angriffen?
5. Wie erfolgen die Angriffe?
6. Wie kann ich mich bzw. mein Unternehmen schützen?
7. Was sollte ich nach einem Schadensereignis tun?

Cybercrime

Bekämpfung in Berlin

Fachdienststellen im Landeskriminalamt Berlin

LKA 24 ZAC zur Zeit eingebettet beim
LKA 245 – qualifizierte Cybercrime im engeren Sinne

Ermittlungsunterstützende Dienststellen (Spezialeinsatztechnik)

Zentrale Ansprechstelle Cybercrime für die Wirtschaft im LKA Berlin

Der Polizeipräsident in Berlin
ZAC – Zentrale
Ansprechstelle Cybercrime

Tel.: 030 - 4664 / 924 924
E-Mail: zac@polizei.berlin.de

Broschüre der ZACs

Download unter

https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/Wirtschaftsunternehmen/wirtschaftsunternehmen_node.html

Eine Überarbeitung findet gerade statt (Februar 2017).

Aktuelle Phänomene

- **Erpressung** im Zusammenhang mit …
  - E-Mails mit Bewerbungen im Cloud-Link oder Schadsoftware im Anhang -> **Verschlüsselungstrojaner**
  - **DDoS-Angriffe** gerade auf Shop-Systeme
  - **Ausgespähte Kundendaten**

- **Ceo-Fraud o. Fake-President**

- **Phishing / Online-Banking**

Beispiele aus der Praxis

- DDoS – Angriff auf ein Shop-System in der Zeit des Hauptumsatzes
- Verschlüsselungstrojaner bei Firma -
  - letztes funktionierendes Backup 2 Jahre alt
  - keine Umsatzsteuererklärung möglich, da Daten nicht wiederherstellbar -> Strafe
  - Patientendaten / Befunde „weg“ …
  - Unterlagen über Forschung nicht „verfügbar“
  - Kundendatenbank verschlüsselt …
  - Nacharbeitung aller Eingaben von X Monaten notwendig
- CEO-Fraud – Überweisung des 2-fachen Jahresumsatzes

Schlagzeilen

Beispiele

Wenn Hacker Krankenhäuser lahmlegen (Gründerszene 18.02.2016)

Hackerangriffe im Krankenhaus – Wo Sicherheitslücken lebensbedrohlich werden
(politik-digital.de 24.03.2016)

Geld her, oder ihr müsst faxen
(zeit.de 18.02.2016)

Wie lange können Sie auf Ihre IT verzichten?

BSI – Die Lage der IT-Sicherheit in Deutschland

Schadprogrammvarianten
- täglich ca. 380.000 neue
- mehr als 560 Millionen bekannt (Stand Aug. 2016)

Zu den Infektionswegen eines Systems mit **Schadprogrammen** gehören
E-Mail-Anhänge
Infektion beim Besuch von Webseiten
Links auf Schadprogramme
Werbebanner („Malvertising“).

Umfrage des BSI:
1/3 der befragten Unternehmen in den letzten 6 Monaten von **Ransomware** betroffen.
3/4 der Infektionen durch infizierte E-Mail-Anhänge
70% einzelne Arbeitsplatzrechner
22% erheblicher Ausfall von Teilen der IT-Infrastruktur
11% verloren wichtige Daten

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=4
DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2016 | GEFÄHRDUNGSLAGE

Typischer Ablauf eines Angriffs und Beobachtungen

Nach einer unbestimmten Zeit der Vorbereitung schafft der Täter es einen beliebigen Computer im Netzwerk zu übernehmen. Ab da dauert es im Schnitt ein bis zwei Tage bis er sich Zugriff auf einen Admin-Account verschaffen konnte.

Je nach Quelle dauert es dann jedoch zwischen 5-8 oder 11-14 Monate bis der unberechtigte Datenabfluss im Unternehmen bemerkt wird.

Vorbereitung – die Frage ist nicht **ob** sondern **wann** Sie angegriffen werden

Sicherheit ist nicht eine Aufgabe der IT-Abteilung sondern der Geschäftsführung!

Sicherheit kostet Geld – allerdings weniger als **ein** Schadensfall

Wer wird angegriffen?

Wir unterscheiden zwei Arten von Unternehmen:

1. die Unternehmen / Organisationen, die bereits angegriffen wurden

2. die Unternehmen / Organisationen, die den Angriff nur noch nicht bemerkt haben ….

Wer greift an?

- 2.3 Angreifer-Typologie
- 2.3.1 Cyber-Kriminelle
- 2.3.2 Nachrichtendienste (z.B. Echolon, PRISM, Tempora, *Evil-Maid*-Attacken)
- 2.3.3 Hacktivismus und Cyber-Aktivisten
- 2.3.4 Innentäter (!)

(BSI-Lagebericht IT-Sicherheit 2014)

Was sind die Ziele der Angreifer?

1. finanzielle Interessen,
2. Informationsbeschaffung,
3. Sabotage,
4. Einflussnahme,
5. Durchsetzung politischer Interessen

Wert von Daten – legal und illegal

Beispiele aus dem Netz

Wie erfolgen Angriffe?

2.2 Angriffsmittel und –methoden

(gestreut) 2.2.1 Spam (-E-Mails)

2.2.2 Schadprogramme

2.2.3 Drive-by-Exploits und Exploit-Kits

(gezielt) 2.2.4 Botnetze

2.2.5 Social Engineering (!)

2.2.6 Identitätsdiebstahl

2.2.7 (Distributed) Denial of Service

2.2.8 Advanced Persistent Threats (APT)

2.2.9 Nachrichtendienstliche Cyber-Angriffe

(BSI-Lagebericht IT-Sicherheit 2014)

Wie erfolgen Angriffe?

bzw. warum sind sie erfolgreich?

2.1 Ursachen

2.1.1 Angriffsplattform Internet

2.1.2 „Digitale Sorglosigkeit“

2.1.3 Schwachstellen (in IT-Produkten)

2.1.4 Einsatz veralteter Software und ungepatchter Systeme

2.1.5 Mobile Endgeräte (BYOD vs. COPE)

2.1.6 Unzureichende Absicherung industrieller Steuerungssysteme

(BSI-Lagebericht IT-Sicherheit 2014)

Suchmaschine Shodan.io

Einfallstore / Fehlerquellen / Datenschutz

- Bedeutung der IT für das Unternehmen
- „Kronjuwelen“ identifiziert und gesichert?
- Passwörter / Benutzerrechte / Werkseinstellung
- Abschottung einzelner Netzwerkteile
- Malware / Einfallstore (Nicht alles muss ins „Netz“)
- Remotezugriff / Fernzugriff bzw. –wartung / Heimarbeitsplätze
- **Backup** (erfolgt regelmäßig? Rückspielung getestet?, Zugriff (auch physikalisch) gesichert?)
- “Bring your own device” (BYOD) vs. COPE (Company owned, personally enabled [MDM (Mobile Device Management)]
- Innentäter / Aussentäter
- Cloud-Computing
- Sorgsamer Umgang mit persönlichen Daten
- Notfallmanagement

N**otfall-Man**agement

Prävention

Detektion

Reaktion

Notfallmanagement - **Prävention**

- Aktuelle Informationen bei kompetenten Partnern einholen
- Informationsschutz als elementaren Bestandteil der Firmenphilosophie und –strategie verankern
- Vor dem Eintreten eines Schadensfalles ein Sicherheitskonzept erstellen
- Ganzheitliches Sicherheitskonzept realisieren und permanent fortschreiben
- Ggfs. Zulieferer / Subunternehmen integrieren
- Kontakt im Vorfeld zu Security-Spezialisten und Ermittlungsbehörden!
- Sicherheitsbewusstsein schaffen z.B. durch Schulung von Mitarbeitern
- Vier-Augen-Prinzip, Need-to-know
- Aktuelle Alarmierungslisten

BSI – Bundesamt für Sicherheit in der Informationstechnik

Auf der Webseite des BSI finden Sie weitere Beispiele zur Anwendung des IT-Grundschutzes:

"**Ein IT-Grundschutzprofil für eine kleine Institution**" ist speziell für die Anwendergruppe mit wenig IT-Systemen und geringen IT-Sicherheitskenntnissen entwickelt worden.

„**Ein IT-Grundschutzprofil für eine große Institution**“ stellt Lösungsvorschläge für häufig auftretende Probleme bei der IT-Grundschutz-Vorgehensweise dar, hier am Beispiel eines Rechenzentrums.

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/WarumITGrundschutz/AufbaudesKurses/aufbaudeskurses_node.html

Notfallmanagement - **Detektion**

- Ganzheitliches Sicherheitskonzept realisieren und permanent fortschreiben
- Sicherheitsstandards regelmäßig analysieren
- Sicherheitsvorkehrungen kontrollieren, Verstöße sanktionieren
- Frühwarnsystem zur Erkennung von Know-How-Verlusten
- Antiviren-Software / Firewall / Intrusion-Detektion / Sandbox / Security Information und Event Management (SIEM) / Anti-Krypto-Programme / Whitelisting v. Exe.
- Security-Monitoring-Konzept (was darf wann von wem protokolliert und ggfs. eingesehen werden?) und Netzwerk-(Traffic)-Analyse

(siehe Broschüre „Wirtschaftsspionage“, Herausgeber: Die Verfassungsschutzbehörden des Bundes und der Länder)

Notfallmanagement - **Reaktion**

- Abarbeitung gemäß zuvor erstellter Handlungsketten
  - Alarmierung(en)
    - IT-Abteilung / ext. IT-Dienstleister
    - Rechtsabteilung / ext. Jurist
    - Firmenleitung / Geschäftsführung
  - ggfs. Hinzuziehung von externen Spezialisten
  - Einschaltung von Strafermittlungsbehörden

Mit dem Zwecke

1. (weiteren) Schaden vom Unternehmen (und deren Kunden) abzuwenden
2. als Unternehmen wieder handlungsfähig zu werden
3. gerichtsverwertbare Beweise zu sichern um den Täter ermitteln und bestrafen zu können

Fazit

IT-Sicherheit ist

1. (leider) notwendig – die Täter werden besser
2. nicht „sexy“ sondern wird immer komplexer
3. Chefsache
4. Teuer (Personal und Material)
5. Aber in aller Regel billiger als **EIN** Schadensereignis!!

„*Standardfragen*“ und meine Antworten

Ab wann ist es ein Angriff, von dem wir als ZAC / Polizei wissen „möchten“?
oder
Was muss / soll ich anzeigen?

Bei Störungen der
Verfügbarkeit, **Integrität**,
Authentizität und
Vertraulichkeit

Quellen

- http://www.bsi.bund.de (IT-Grundschutz),
- http://www.heise.de/security/
- www.bitkom.org,
- www.funkschau.de,
- ww.datensicherheit.de
- Microsoft
- https://assets.kpmg.com/content/dam/kpmg/pdf/2016/07/wirtschaftskriminalitaet-2016-2-KPMG.pdf
- Computer Forensik, Alexander Geschonneck, dpunkt.verlag 5. Aufl. 2011

Zentrale Ansprechstelle Cybercrime für die Wirtschaft im LKA Berlin

Der Polizeipräsident in Berlin
ZAC – Zentrale
Ansprechstelle Cybercrime

Tel.: 030 - 4664 / 924 924
E-Mail: zac@polizei.berlin.de