Cyber Crime

Gefahren, Bedrohung, Ursachen, Massnahmen

KZEI Fyrabig-Anlass vom 22. März 2018

Oliver Hunziker, 52
Informatiker seit 1985

Heute:

- Abteilungsleiter ICT
- IT-Consultant für KMU
- Private-Cloud-Spezialist
- IT-Security-Berater

oh@reich-nievergelt.ch
+41 44 283 4014

Reich + Nievergelt AG

- Gegründet 1973 durch Walter Nievergelt und Ernst Reich
- Heute rund 45 Mitarbeiter
- Verankert in Zürich 2 seit der Gründung
  Heute: Waffenplatz / Brandschenkestrasse 178

Haupttätigkeiten

- Starkstrom für Neu- und Umbauten
- Telematik, Netzwerktechnik, Alarm und Sicherheit
- Informatik, Kommunikation, ICT

Reich + Nievergelt AG
Brandschenkestrasse 178
8002 Zürich
+41 44 201 0909
www.reich-nievergelt.ch
info@reich-nievergelt.ch

Hauptformen von Cyberkriminalität

Phishing

Kriminelle bringen Passwörter in Erfahrung – zum Beispiel mit gefälschten Mails oder Websites. Auch an weiteren persönlichen Daten sind sie interessiert. Damit können sie im Namen des Opfers Geschäfte abwickeln.

Ransomware

Eine Schadsoftware blockiert den Computer. Es erscheint eine vermeintlich behördliche Mitteilung die zur Bezahlung einer Busse auffordert, damit der Computer wieder entsperrt wird.

Spyware

Spyware wird eingesetzt, um Passwörter und Zugangsdaten zu erhalten. Spyware wird oft beim Surfen auf Websites übertragen, durch Herunterladen von Software oder Öffnen von infizierten Anhängen. Aber auch durch Öffnen einer Datei von einem Datenträger.

Encryption

Verschlüsselungssoftware wird via Trojaner ausgeliefert und verschlüsselt die Daten auf den Systemen. Entschlüsselung nur gegen Lösegeldzahlung möglich.

Andere Formen von Cyberkriminalität

Romance Scam
Gefälschte Profile auf Singlebörsen. Hauptsächlich verwendet um Geld zu erpressen

Sextorsion
Opfer wird auf Videoplattformen zu sexuellen Handlungen verführt und danach mit dem Material erpresst.

DDOS-Angriff
Attackiert Server und legt sie lahm. Kann Web- oder Mailserver sowie Onlineshops lahmlegen und damit Firmen
Schaden zufügen.

Identitätsdiebstahl
Fremde beschaffen sich durch gefälschte Freundschaftsanfragen Informationen. Auch als Social-Engineering bekannt und verwendet.

Sowie weitere Varianten der genannten Formen

Phishing

Hauptsächlich über gefälschte E-Mails.
Häufig verwendet bei:

- Banken, Post
- Swisscom
- Mailportale
- Bestellportale (Zalando, Amazon etc)

Ziel

- **Zugriff auf das Konto**
- **Diebstahl von Geld**
- **Zugriff auf Firmensysteme**
- **Sammeln von Zugangsdaten**

Ransomware

Angebliche Blockierung des Computers
Mit Erpressungsforderung (Busse)

Häufig technisch sehr trivial
Schaden trotzdem erheblich

Ziel

- **Erpressung**
- **Lahmlegen von Unternehmen/Personen**

Spyware

Meist durch sogenanntes «DriveBy» von infizierten Websites heruntergeladen.
Aber auch durch Download von angeblichen Sicherheits- oder Tuningprogrammen.

Quelle muss nicht «dubios» sein, kann auch einfach infiziert sein.

Ziel

- **Diebstahl von Geld**
- **Zugriff auf Firmensysteme**
- **Sammeln von Zugangsdaten**

Encryption

Häufig durch Trojaner (Ransomware) eingeschleppt.
Verschlüsselt alle Dateien auf allen erreichbaren Laufwerken.

Achtung:
Je nach Backupsystem können auch Backups betroffen sein.

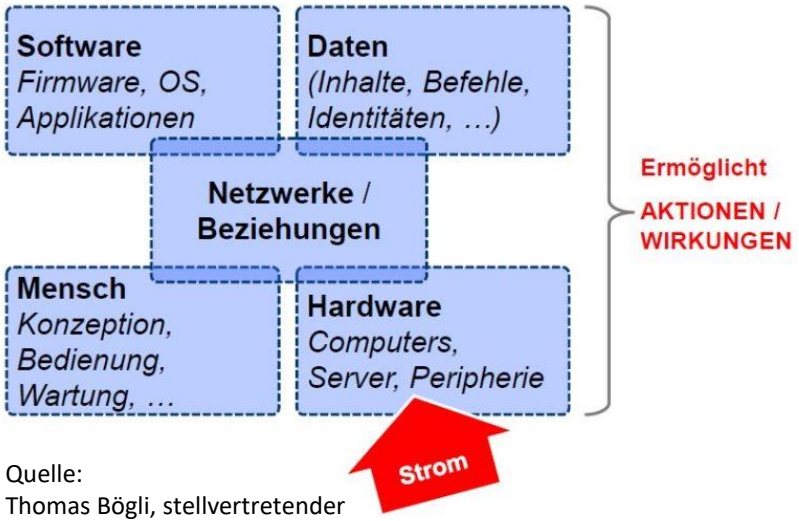
Ziel

- **Erpressung (Hohe Beträge (x-Tausend)**

Risikozonen

1. **Vernachlässigung elementarer IT-Security**
   - Keine oder mangelhafte Passwörter
   - Keine Firewall, kein Antivirus oder veraltet
   - «Lose Enden» in der Netzwerkstruktur
   - Unsichere WLAN-Konfigurationen

2. **Mangelnde Information der Mitarbeiter**
   - Benutzer sind nicht informiert über Risiken
   - Benutzer haben zu hohe IT-Rechte



Quelle:
Thomas Bögli, stellvertretender
Leiter Cyber-Defence der Schweizer Armee

Gegenmassnahmen

- Umfassendes BCM gegen den Verlust der Verfügbarkeit
  (BCM: Business Continuity Management)
- Umfassende Verschlüsselung gegen den Verlust der Vertraulichkeit
- Umfassende Nachvollziehbarkeit gegen den Verlust der Integrität
- Konsequente Mehrfaktoren-Authentifizierung
- Schwachstelle Mensch

Quelle: Thomas Bögli, stellvertretender Leiter Cyber-Defence der Schweizer Armee

Verhaltensregeln

Passwörter

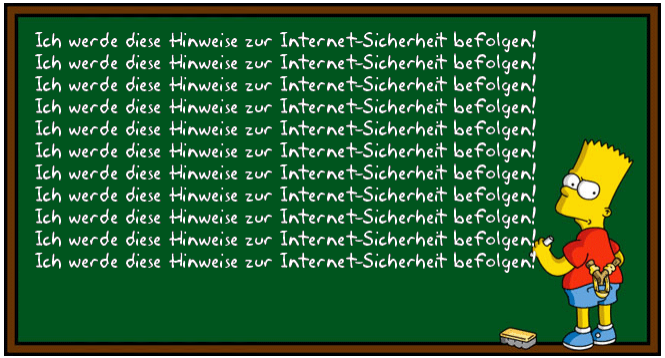
- Sichere Passwörter (mindestens 8 Zeichen inkl. Sonderzeichen
- Keine Mehrfachnutzung von Passwörtern
- Passwörter regelmässig ändern

E-Mail

- Misstrauen Sie E-Mails mit unbekannten Absenderadressen.
- Keine Anhänge von unbekannten oder suspekten Absendern öffnen
- Vorsicht bei ausführbaren Anhängen (doc,xls,exe,vbs etc)
- Spam nie beantworten (keine «Abmeldung» vom Newsletter)

Internet

- Keine unbekannten Programme herunterladen/installieren
- Vorsicht bei der Weitergabe von Informationen (Social Engineering)
- Immer korrekt abmelden von Websites.



Quelle: MELANI

Technische Massnahmen in der IT:

Netzwerkschutz

- Aktuelle, leistungsfähige Firewall
- Webfilterung, AntiSpam-Massnahmen, Antivirus, Intrusion-Protection
- Netzwerk wenn möglich gekapselt (unterschiedliche Bereiche)

Zugangsschutz

- Physischer Schutz der sensitiven Anlagen (Server etc)
- Sichere Verwahrung von Masterpasswörtern

Kontrolle

- Regelmässige Überprüfung der getroffenen Massnahmen

Mit vertretbarem Aufwand die Sicherheit erhöhen, ohne dabei die Usability zu beeinträchtigen.

Wichtige Informationsquellen

MELANI
Melde- und Analysestelle Informationssicherung
www.melani.admin.ch

FEDPOL
Bundesamt für Polizei Fedpol
www.fedpol.admin.ch

Fachstelle Cybercrime Kantonspolizei Zürich
www.kapo.zh.ch

Schweizerische Kriminalprävention
www.skppsc.ch/de/themen/internet

Wer hilft?

Cyber Crime


ICT
› ICT Consulting
› ICT Outsourcing
› Cloud-Lösungen
› Mail Security
› Virtualisierungen
› Backup-Lösungen

Cyber Crime

Herzlichen Dank
für Ihre Aufmerksamkeit

Oliver Hunziker, 52
Informatiker seit 1985
Heute:

- Abteilungsleiter ICT
- IT-Consultant für KMU
- IT-Security-Berater

oh@reich-nievergelt.ch
+41 44 283 4014

REICH+NIEVERGELT AG

http://www.reich-nievergelt.ch/ict