Kanton Zürich
Amt für Informatik

Cybersicherheit in KMU: Aktuelle Bedrohungen und Schutzmechanismen

Benedikt Meier, Programm Manager Cybersecurity
Sascha Schönauer, Security Consultant



Guess what! Cyber Crime Facts



… Zunahme der Cyberangriffe auf Schweizer Unternehmen (NCSC)

… so schnell kann ein nicht gepatchtes System nach Online-Stellen von Angreifern erkannt und angegriffen werden.

... durch-schnittlicher Schaden für einen schweren Cyber-Angriff auf ein Schweizer KMU.

… weltweit zielen auf KMU – weil sie oft schlechter geschützt sind.

… der betroffenen KMU stellen ihre Geschäfts-tätigkeit innerhalb von 6 Monaten nach einem schweren Cyberangriff ein (weltweit).

… der Sicherheits-vorfälle sind auf menschliches Fehlverhalten zurückzuführen (z. B. schwache Passwörter, Phishing-Klicks).

… der Schweizer KMU haben keinen Notfallplan für Cyberangriffe

Agenda

- **Input Teil 1: Angriff**
- **Break Out Session**
- **Input Teil 2: Verteidigung**
- **Break Out Session**
- **Konkrete Hilfsmittel**

Agenda

- **Input Teil 1: Angriff**
  - Wer greift mich an? Hackertypen
  - Womit werde ich angegriffen? Werkzeuge für Angriffe
  - Wie werde ich angegriffen? The Cyber Kill Chain
- **Break Out Session**
- **Input Teil 2: Verteidigung**
- **Break Out Session**
- **Konkrete Hilfsmittel**

Input Teil 1 - Offence



Wer greift mich an?

Top 5 Angreifer



Black Hat

Krimineller Hacker

handeln illegal, stehlen, erpressen, zerstören



Insider Threats

Mitarbeitende (ex oder aktuell)

haben böse Absichten oder handeln nachlässig



Script Kiddies

Unerfahrene Hacker

nutzen fertige Tools – meist ohne tiefes Wissen und «just for fun»



Hacktivists

Aktivisten

politisch oder ideologisch motivierte Gruppen

(z. B. Anonymous)



State-sponsored

“der Beamte”

von Staaten unterstützte Hackergruppen

(z. B. für Spionage, Sabotage)

Womit werde ich angegriffen?

Top 5 Werkzeuge der Angreifer



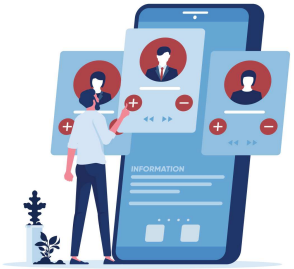
Phishing

Gefälschte E-Mails/Webseiten zur Passwortabfrage oder Malware-Verbreitung



Malware / Ransomware

Schadsoftware, die Systeme lahmlegt oder Daten verschlüsselt



Social Engineering

Manipulation von Mitarbeitenden zur Abgabe von Zugangsdaten oder zur Ausführung gefährlicher Aktionen



Exploits (Zero-Day oder bekannte Schwachstellen)

Ausnutzung technischer Sicherheitslücken in Software/Hardware



DDoS Angriffe

Überlastung von Webservern oder Diensten durch massenhafte Anfragen (meist aus Botnets)

Wie werde ich angegriffen?

The Cyber Kill Chain – Lockheed Martin

Ausnutzung (Exploitation)
Die zuvor identifizierte Schwachstelle wird genutzt, um sich initialen Zugang zu sichern.

Gezielter Angriff (Delivery)
Ein gezielter Angriff findet statt via Phishing, das Netzwerk oder ein physisches Medium.

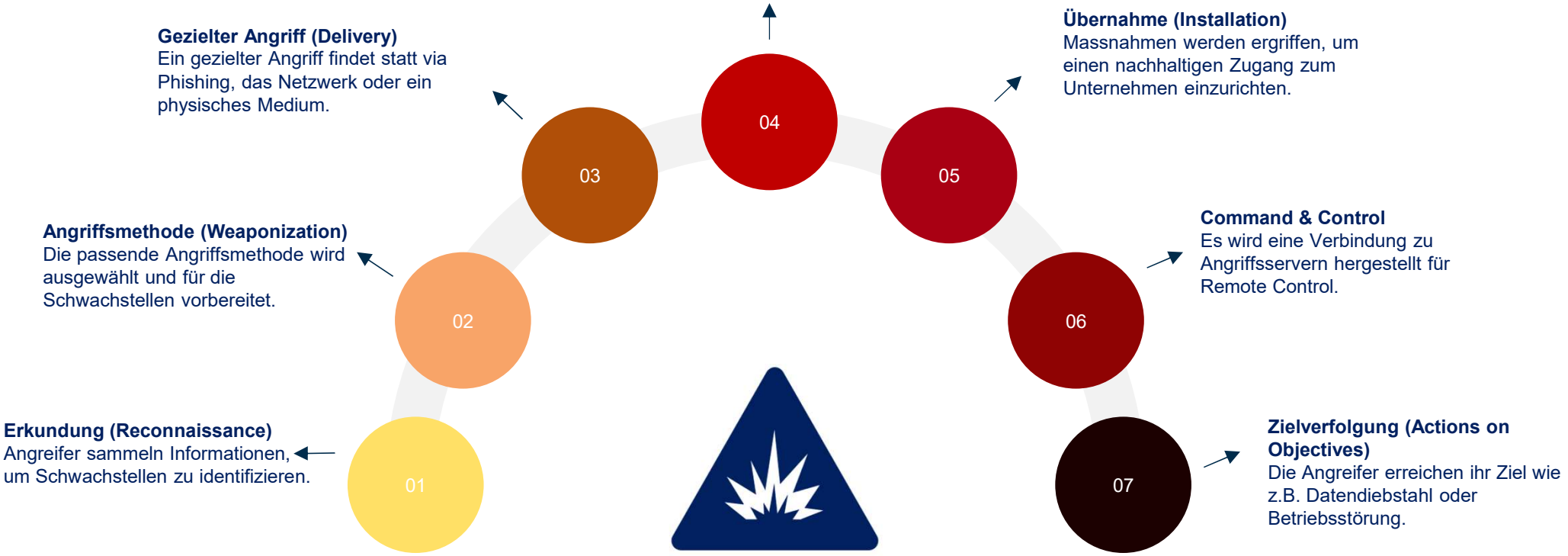
Übernahme (Installation)
Massnahmen werden ergriffen, um einen nachhaltigen Zugang zum Unternehmen einzurichten.

Angriffsmethode (Weaponization)
Die passende Angriffsmethode wird ausgewählt und für die Schwachstellen vorbereitet.

Command & Control
Es wird eine Verbindung zu Angriffsservern hergestellt für Remote Control.

Erkundung (Reconnaissance)
Angreifer sammeln Informationen, um Schwachstellen zu identifizieren.

Zielverfolgung (Actions on Objectives)
Die Angreifer erreichen ihr Ziel wie z.B. Datendiebstahl oder Betriebsstörung.



Agenda

- **Input Teil 1: Angriff**
- **Break Out Session**
  - Wir greifen an
- **Input Teil 2: Verteidigung**
- **Break Out Session**
- **Konkrete Hilfsmittel**

Break-Out Session:
Wir greifen an

2 Aufgaben:
- Linke Seite des Raums: Aufgabe 1
- Rechte Seite des Raums: Aufgabe 2

Gruppen:
- Finden Sie sich in Gruppen von 2-5 Personen zusammen
- Scannen sie den QR Code und besprechen Sie die gestellten Aufgaben

Auflösung:
- Präsentation der Auflösung im Anschluss
- Kurze Möglichkeit für Q&A

Break-Out Session: Wir greifen an

Aufgabe 1 – Probana

Anhang A

Aufgabe 2 – NexVoice

Anhang B

Auflösung Probana / Fasana



Auflösung Nexvoice / 3CX



Agenda

- **Input Teil 1: Angriff**
- **Break Out Session**
- **Input Teil 2: Verteidigung**
  - Top 5 Massnahmen
- **Break Out Session**
- **Konkrete Hilfsmittel**

Input Teil 2 - Defence



Quelle:
Image by zsclions - Grosse Paraden, grosses Herz | ZSC Lions

Top 5 Massnahmen



Schulung der Mitarbeitenden

Regelmässige Awareness-Trainings



Sichern der Mitarbeiter-zugriffe

Nutzen der Möglichkeiten von zusätzlicher Authentifizierung (MFA)



Regelmässige Updates & Patching

Betriebssysteme, Server, Software und Geräte stets aktuell halten



Backups & Offline Kopien

Tägliche Backups, mind. 1x pro Woche offline speichern



Überwachung und Notfallplan

Klarer Plan: Wer macht was im Angriffsfall? Enthält Kontakte, Abläufe, externe Partner

Agenda

- **Input Teil 1: Angriff**
- **Break Out Session**
- **Input Teil 2: Verteidigung**
- **Break Out Session**
  - Wir verteidigen
- **Konkrete Hilfsmittel**

Break-Out Session:
Wir verteidigen

2 Aufgaben:

- Linke Seite des Raums: Aufgabe 1
- Rechte Seite des Raums: Aufgabe 2

Gruppen:

- Finden Sie sich in Gruppen von 2-5 Personen zusammen
- Scannen sie den QR Code und besprechen Sie die gestellten Aufgaben

Auflösung:

- Präsentation der Auflösung im Anschluss
- Kurze Möglichkeit für Q&A

Break-Out Session:
Wir verteidigen

Gruppe 1 – FASANA

Anhang C

Gruppe 2 - 3CX

Anhang D

Auflösung Fasana

Krise meistern

- Überblick über den Angriff
- Status der Backups
- Auswirkungen auf das Geschäft (Produktion, Verwaltung, Kommunikation)?
- Kommunikation. Wer informiert Mitarbeitende, Kunden, Lieferanten und Behörden?
- Gibt es einen Krisenkommunikationsplan?

Auflösung Fasana

Wie hätte es verhindert werden können?

Technische Massnahmen	Organisatorische Massnahmen	Erste Schritte im Ernstfall
Netzwerksegmentierung	Notfallplan	Netzwerk trennen
Air-Gapped Backups	Phishing-Simulationen	Backups prüfen & ggf wiederherstellen
Echtzeitüberwachung (SIEM)	Regelmässige Audits	Krisenstab aktivieren

Auflösung 3CX

Krise meistern

- Betroffene Systeme isolieren
- IT-Forensik und Incident Response aktivieren
- Backups prüfen
- Krisenstab und Kommunikation sicherstellen

Auflösung 3CX

Wie hätte es verhindert werden können?

Technische Massnahmen	Organisatorische Massnahmen	Erste Schritte im Ernstfall
Monitoring & Alarmierung	Regelmässige Awareness	Netzwerk sofort trennen
Zero Trust-Prinzip	Klare Notfallpläne	Backups prüfen & ggf. wiederherstellen
Multi-Faktor-Authentifizierung	Regelmässige Tests (Notfallszenario)	Krisenstab aktivieren

Agenda

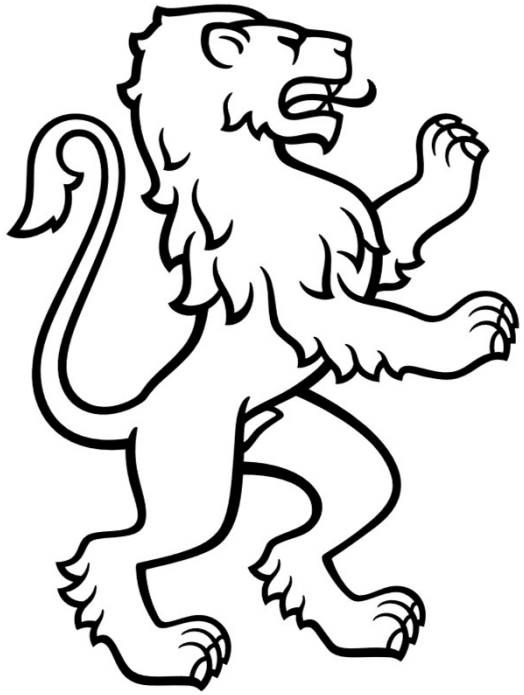
- **Input Teil 1: Angriff**
- **Break Out Session**
- **Input Teil 2: Verteidigung**
- **Break Out Session**
- **Hilfsmittel**
  - Hilfsmittel
  - CYREN – Cybersecurity Clinic

Hilfsmittel

Offizielle Leitlinien, technische Checklisten, rechtliche Anforderungen	https://www.ncsc.admin.ch/	**Bundesamt für Cybersicherheit BACS**
KMU-Checks, Sensibilisierung, Dienstleisternetzwerk	https://itsec4kmu.ch/	IT Sec 4 KMU
Auswahl von Standard-rahmenwerken via Online-Tool	https://cybernavi.ch/	cybernavi
Awareness-Themen, Sicherheitschecks, leicht verständlich	https://www.ibarry.ch/de	iBarry

CYRENZH Cybersecurity Clinic





Kanton Zürich

Quellen

– Guess what – Folie 2

Topic by
Cyberstudie 2024 – IT-Sicherheit in Schweizer KMU, bei IT-Dienstleistungsunternehmen und in der Schweizer Bevölkerung
Hack-Angriff: Ransomware-Gruppe Play erpresst NZZ und CH Media – Blick
Warum Cybersecurity für Schweizer KMU unverzichtbar ist

– Input Teil 1 – Offence – Folie 4

Image by AI http://www.canva.com/

– Auflösung Probana / Fasana – Folie 14

Image by Cybernews German napkin factory insolvent following cyberattack | Cybernews
Topic by Nach über 100 Jahren: Cyberangriff drängt deutsche Firma in die Insolvenz - Golem.de

– Auflösung NexVoice / 3CX Folie 16

Image by bitdefender - Technical Advisory: Software Supply Chain Attack Against 3CX Desktop App
Topic by darktrace - Darktrace Detection of 3CX Supply Chain Attack

– Input Teil 2 – Defence – Folie 19

Image by zsclions - Grosse Paraden, grosses Herz | ZSC Lions

Anhang A

Angriffsvorbereitung auf Probana

Sie sind Teil eines Hacker-Teams, das gezielt nach lukrativen Zielen für einen Cyberangriff sucht. Ihre Aufmerksamkeit fällt auf die Probana GmbH – ein traditionsreiches, mittelständisches Unternehmen und einer der grössten Serviettenhersteller Europas. Probana produziert seit über 100 Jahren, beschäftigt rund 200 Mitarbeitende und beliefert grosse Handelsketten im In- und Ausland. Das Unternehmen verfügt über eine moderne, digitalisierte Produktion und eine zentrale IT-Infrastruktur, die Verwaltung, Produktion und Logistik miteinander verbindet.

Probana weist die typischen Schwachstellen eines KMUs auf: veraltete Systeme, mangelnde Segmentierung, fehlende Awareness bei Mitarbeitenden und unzureichende Backups.

Ihre Aufgabe

Versetzen Sie sich in die Rolle der Angreifer: Ziel ist es, mögliche Sicherheitslücken eines mittelständischen Produktionsunternehmens systematisch auszunutzen, um mit möglichst geringem Aufwand maximalen Schaden zu verursachen oder hohe Lösegeldforderungen durchzusetzen. Wie würden sie im Falle von Probana vorgehen (anhand der Cyber Kill Chain) und welche Werkzeuge würden sie dafür einsetzen?

Welche Folgen hätte ein solcher Angriff für Probana, seine Kunden und seine Lieferanten? Betrachten Sie dies sowohl technisch (z.B. Produktionsausfall, Datenverlust) als auch wirtschaftlich (z.B. Umsatzeinbussen, Reputationsverlust, mögliche Insolvenz).

Anhang B

Angriff auf Nexvoice als Grossunternehmen

Ihr Hacker-Team hat es geschafft, in das Netzwerk des Softwareanbieters Nexvoice einzudringen. Nexvoice ist ein international tätiges Softwareunternehmen, das auf internetbasierte Telekommunikationslösungen spezialisiert ist. Das Unternehmen wurde 2005 gegründet und ist vor allem bekannt für seine VoIP-Telefonanlage (IP-PBX), die Unternehmen ermöglicht, ihre Telefonie über das Internet abzuwickeln. Ihrem Team ist es gelungen, die Software Entwicklung und Bereitstellung zu kompromittieren. Dadurch können Sie Schadcode in offiziell signierte Updates der Nexvoice Desktop App einschleusen, die weltweit von über 600.000 Unternehmen und Millionen von Nutzern eingesetzt wird. Die Kontrolle über Nexvoice ist gesichert – Sie entscheiden, wie Sie diesen Zugang nutzen.

Ihre Aufgabe:

Fokussieren Sie sich auf Ihre Rolle als Angreifer und überlegen Sie, welche Optionen Ihnen nach der erfolgreichen Kompromittierung eines so zentralen Softwareanbieters offenstehen. Diskutieren Sie, wie Sie Ihre Position in der Lieferkette nutzen wollen, anstatt sich nur auf die Erpressung von Nexvoice selbst zu beschränken. Welche Angriffsziele könnten für Sie am lukrativsten sein?

Bewerten Sie die Risiken und Chancen verschiedener Angriffswege (z.B. Datendiebstahl, Ransomware Erpressung, Industriespionage, Weiterverbreitung von Malware an die Kunden von Nexvoice, Aufbau eines Botnetzes (z.B. für DDoS Attacken), gezielte Angriffe auf besonders wertvolle Endkunden). Wie würden Sie Ihre Möglichkeiten nutzen und warum?

Anhang C

Fallbeispiel 1: Fasana
Wie ein Cyberangriff ein Traditionsunternehmen auslöschen kann

Nachdem Sie zuvor das Szenario „Probana“ bearbeitet haben, finden Sie hier nun die Informationen zur realen Geschichte:
Am 19. Mai 2024 wurde der Traditionshersteller Fasana Ziel eines gezielten Ransomware-Angriffs. Plötzlich standen alle 190 Systeme und Maschinen still, 240 Mitarbeitende konnten weder produzieren noch kommunizieren – sogar die Erpresser-Botschaft kam direkt aus den Druckern. Die Produktion lag zwei Wochen komplett brach, der Schaden wuchs auf rund 2 Millionen Euro, pro Tag gingen über 250.000 € Umsatz verloren. Am 1. Juni blieb nur noch der Insolvenzantrag – ein über 100 Jahre altes Unternehmen wurde durch einen einzigen Cyberangriff existenzbedrohend getroffen

Aufgabenstellung für Gruppe 1:

Krise meistern

Welche Informationen brauchen Sie dringend in einer solchen Krisensituation, um die Lage zu beurteilen und die nächsten Schritte zu planen?
Was wären die allerersten Schritte, die Sie tun müssen, um den Schaden zu begrenzen und auf den Vorfall zu reagieren?

Krise verhindern

Welche präventiven technischen Massnahmen wären sinnvoll gewesen, um den Angriff zu verhindern oder seine Auswirkungen drastisch zu mindern?
Welche Rolle spielen organisatorische Massnahmen (z.B. Mitarbeiter-Sensibilisierung, interne Richtlinien, Notfallpläne) bei der Prävention?

Anhang D

Fallbeispiel 2: Die stille Gefahr
Wenn der Zulieferer zum Einfallstor wird

Nachdem Sie zuvor das Szenario „Nexvoice“ bearbeitet haben, folgt nun das reale Beispiel:
Im Frühjahr 2023 wurde die weit verbreitete 3CX DesktopApp Opfer eines hochkomplexen Supply-Chain-Angriffs. Nicht 3CX selbst, sondern ein Zulieferer – Trading Technologies – wurde kompromittiert: Eine manipulierte Version der Software „X_TRADER“ öffnete den Angreifern (Lazarus-Gruppe, Nordkorea) den Weg. Über diesen Umweg gelang es ihnen, Schadsoftware in die offiziell signierten Updates der 3CX-App einzuschleusen. Weltweit installierten Tausende Unternehmen unwissentlich eine Backdoor, die sensible Daten wie Zugangsdaten und Browser-Informationen abgriff und weitere Schadsoftware nachladen konnte – ein Angriff, der zeigte, wie gefährlich und schwer zu erkennen Schwachstellen in der Lieferkette sind.

Aufgabenstellung für Gruppe 2:

Krise meistern

Welche Informationen brauchen Sie dringend in einer solchen Krisensituation, um die Lage zu beurteilen und die nächsten Schritte zu planen?
Was wären die allerersten Schritte, die Sie tun müssen, um den Schaden zu begrenzen und auf den Vorfall zu reagieren?

Krise verhindern

Welche präventiven technischen Massnahmen wären sinnvoll gewesen, um den Angriff zu verhindern oder seine Auswirkungen drastisch zu mindern?
Welche Rolle spielen organisatorische Massnahmen (z.B. Mitarbeiter-Sensibilisierung, interne Richtlinien, Notfallpläne) bei der Prävention?