FFHS
Fernfachhochschule Schweiz
Mitglied der SUPSI

Cyber Resilience

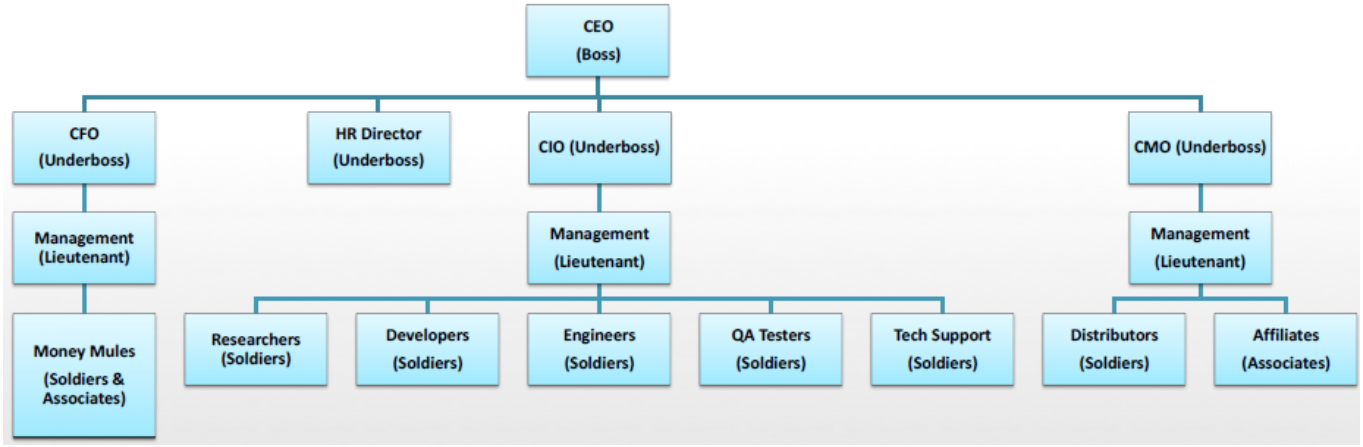
Warum Cyber Security nicht mehr ausreicht?

Christian Thiel, **"iischi Wirtschaft"**

Cybercrime Inc. – Professionalisierung des Cyber Crime

- 80% der Hacker arbeiten mit der organisierten Kriminalität zusammen.
  - Cosa Nostra, Japanische Yakuza, Chinesische Triaden, Russische Mafia, Südamerikanische Kartelle,…

- Cyberkriminalitätsorganisationen
  - "businessorientiert"
  - gut organisiert
  - Unternehmensstrategien
  - Anonymitätsmethoden:
    - Darknet
    - Kryptowährungen



Ablauf einer zielgerichteten Attacke

Präparierte Webseite

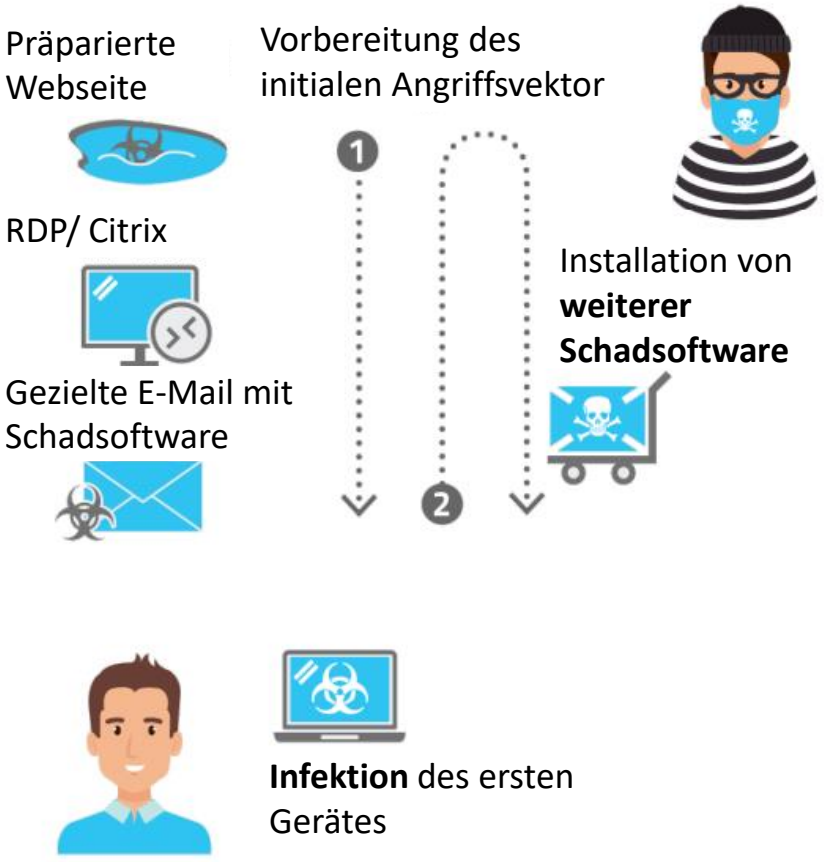
RDP/ Citrix

Gezielte E-Mail mit Schadsoftware

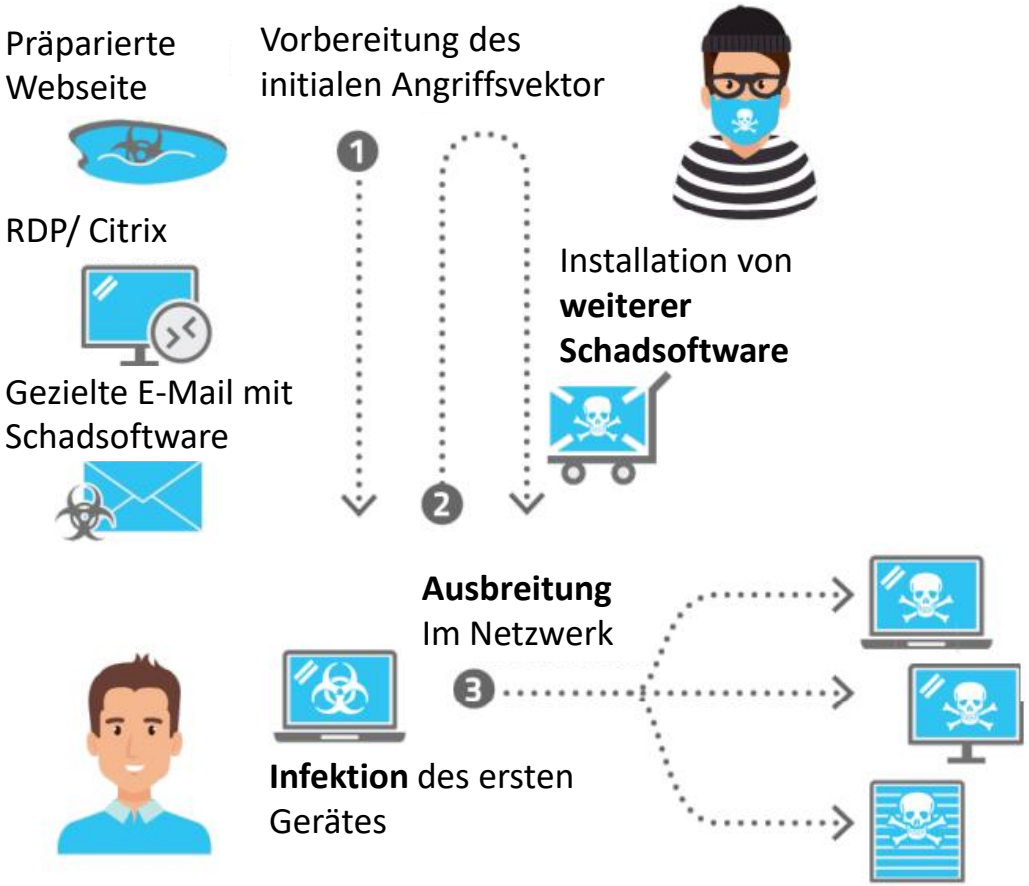
Vorbereitung des initialen Angriffsvektor

Infektion des ersten Gerätes

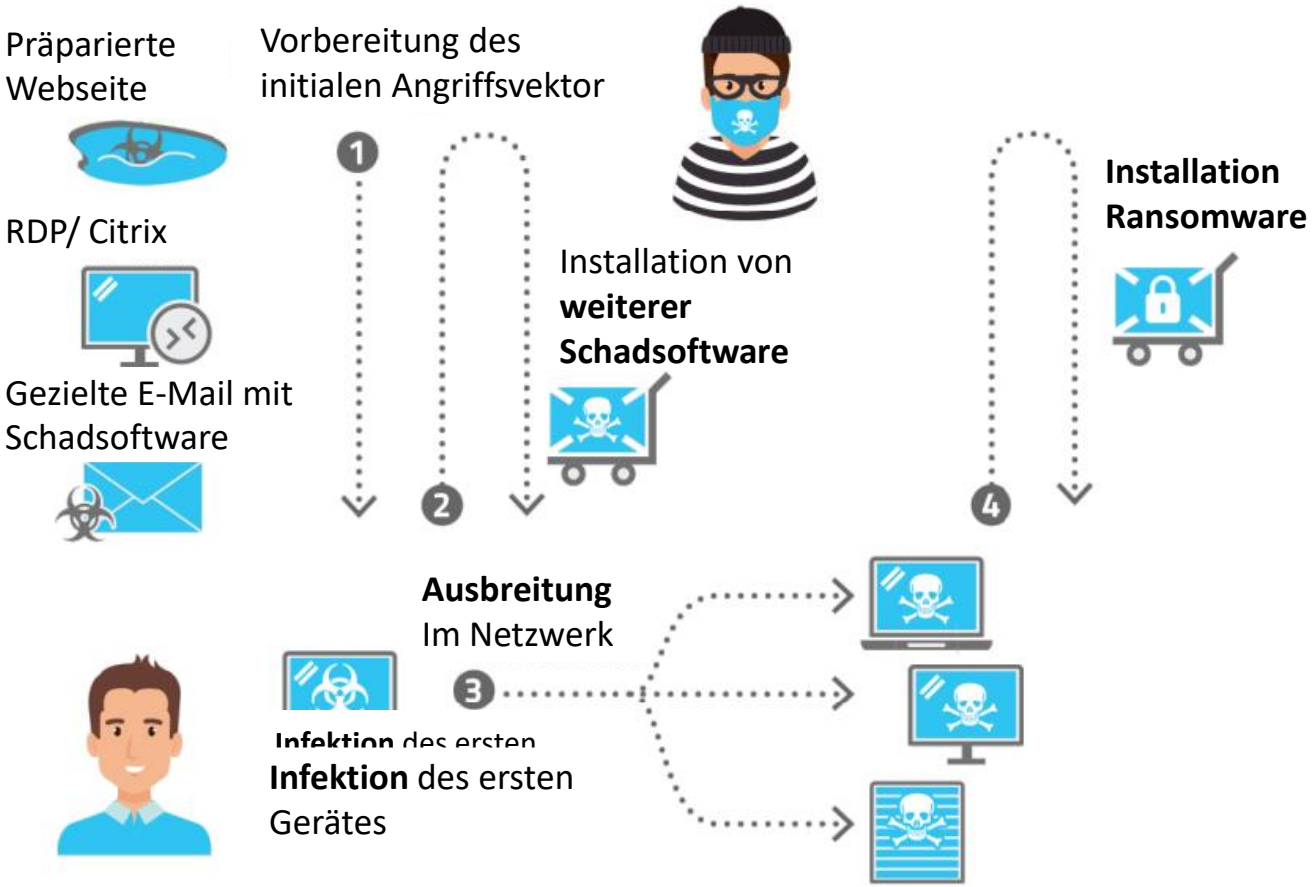
Ablauf einer zielgerichteten Attacke



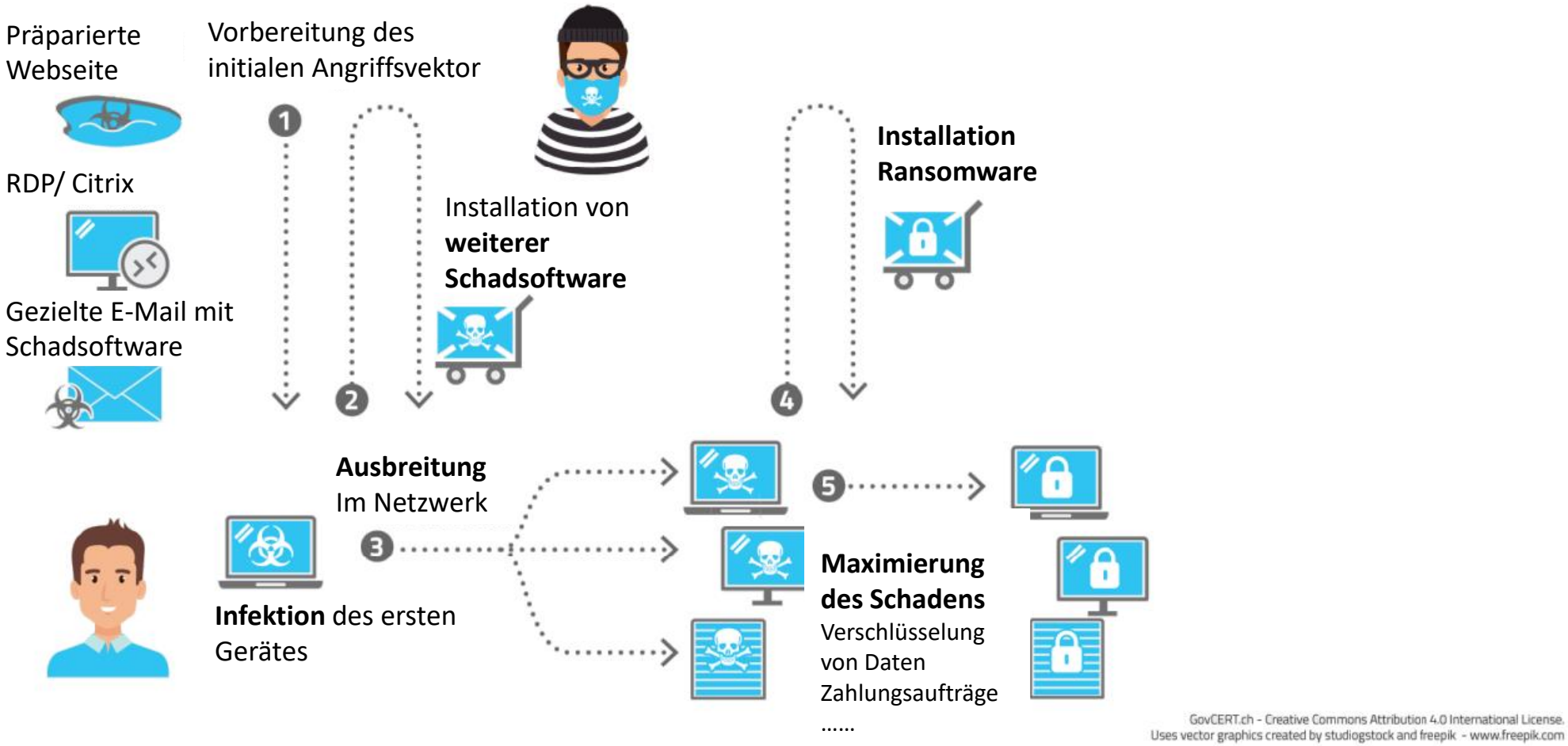
Ablauf einer zielgerichteten Attacke



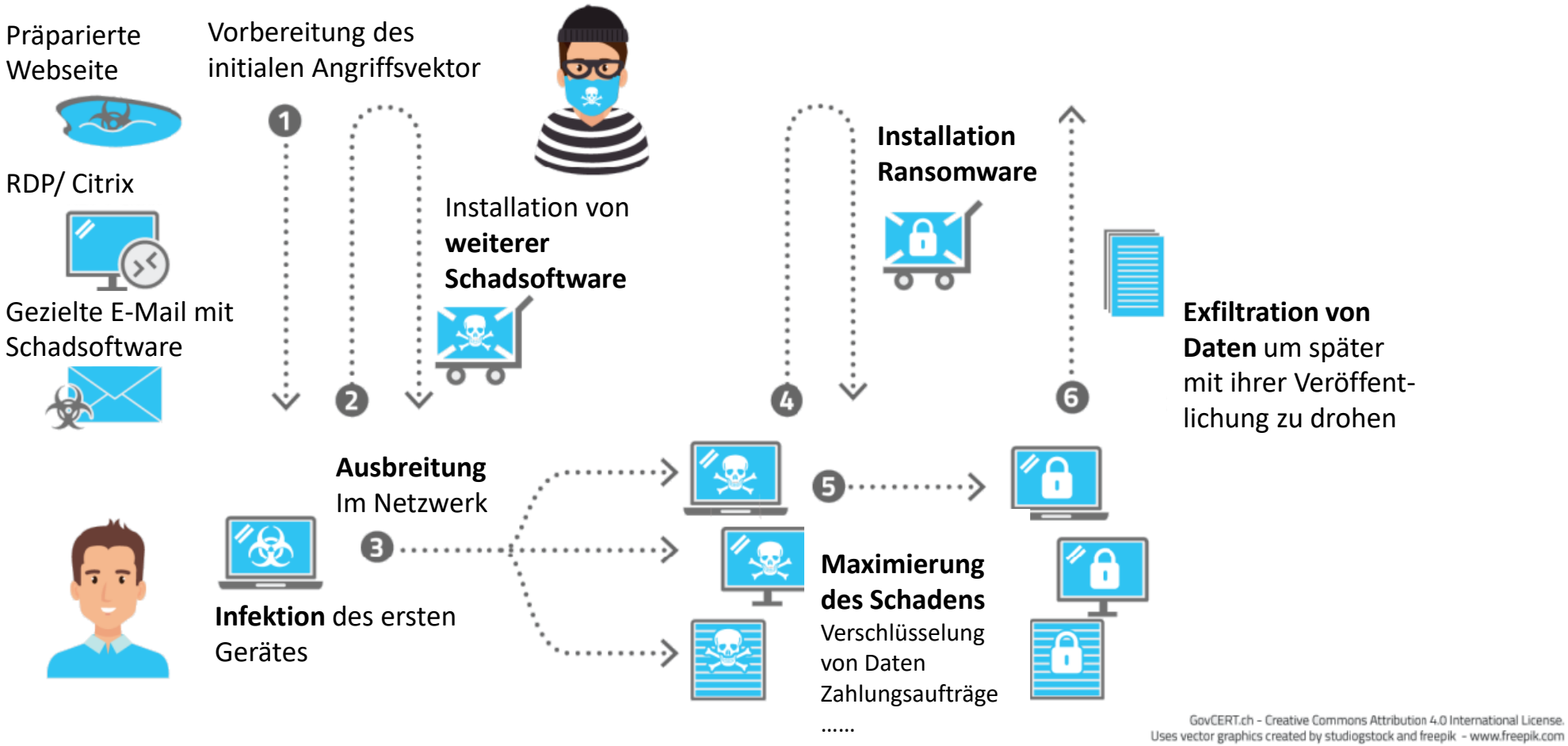
Ablauf einer zielgerichteten Attacke



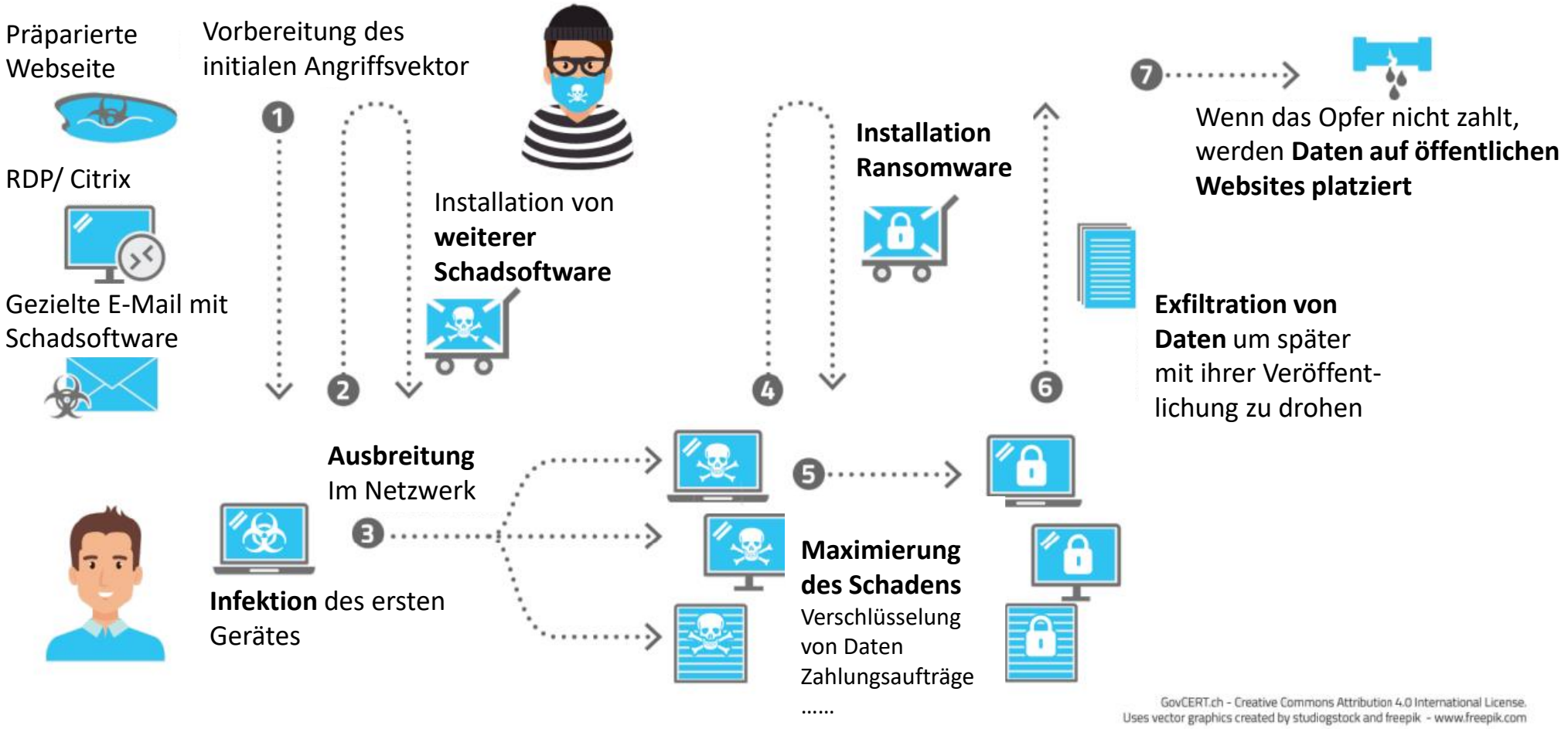
Ablauf einer zielgerichteten Attacke



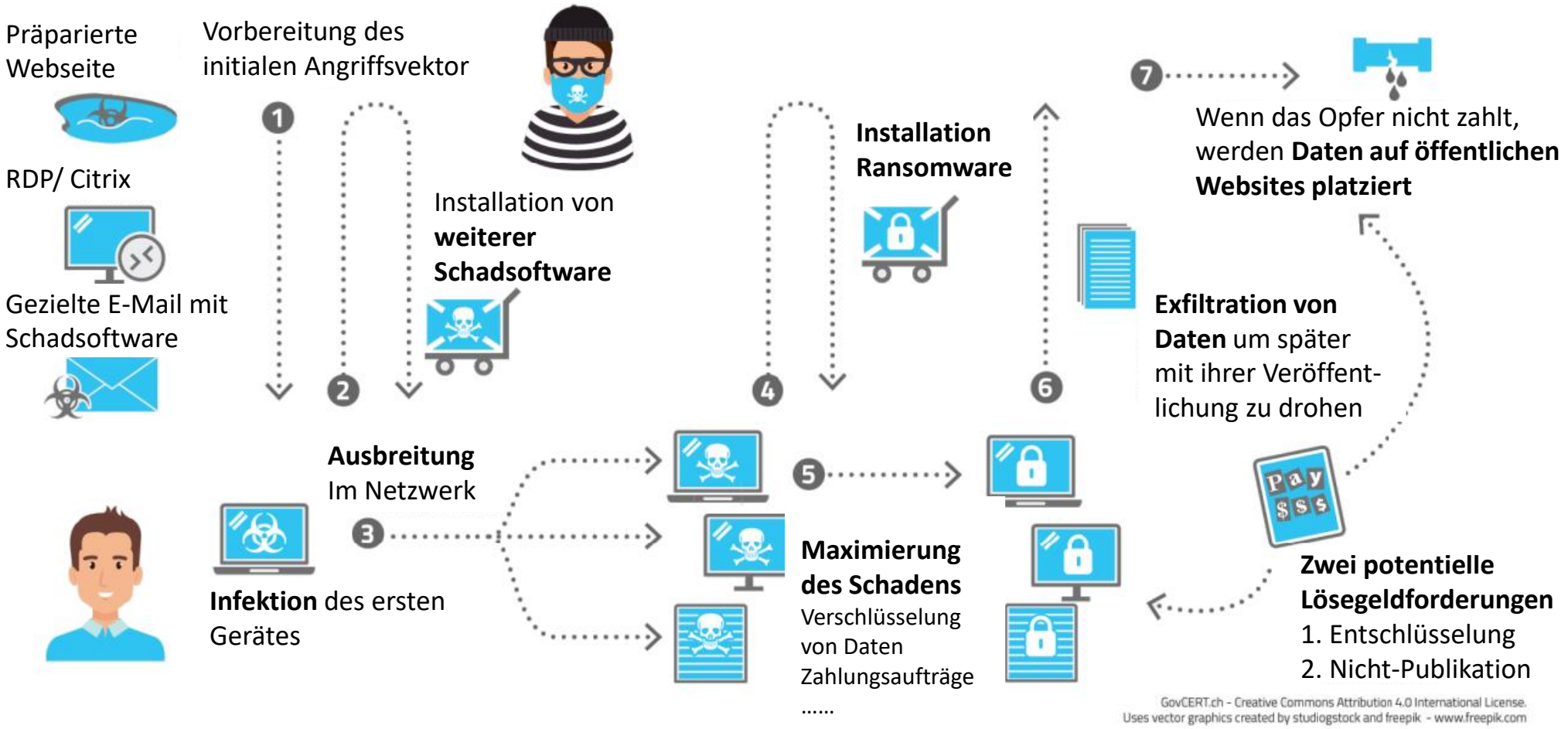
Ablauf einer zielgerichteten Attacke



Ablauf einer zielgerichteten Attacke



Ablauf einer zielgerichteten Attacke



Wichtige Basisschritte zu besser Cyber Security

1. Sichern Sie Ihre Daten regelmässig mit Backups
2. Halten Sie Ihr Antivirus-Programm aktuell
3. Schützen Sie Ihren Internetzugang
4. Aktualisieren Sie Ihre Software regelmässig
5. Verwenden Sie starke Passwörter
6. Schützen Sie Ihre mobilen Geräte
7. Machen Sie Ihre IKT-Benutzerrichtlinien bekannt
8. Schützen Sie die Umgebung Ihrer IKT-Infrastruktur
9. Regeln Sie den Zugriffschutz auf Daten
10. Verschlüsseln Sie mobile Datenträger und Übermittlung
11. Sensibilisieren Sie ihre Mitarbeitenden
12. Regeln Sie die Entsorgung von Informationen und Informationsträgern
13. Überprüfen Sie Ihre Systeme
14. Schützen Sie den Zugang in Ihr Firmennetz durch eine Zwei-Faktor-Authentifizierung
15. Sorgen Sie für eine unterbruchsfreie Stromversorgung
16. Halten Sie wichtige Elemente redundant
17. Planen Sie die Notfallvorsorge
18. Verteilen Sie das Know-How

Verbesserung der Cybersicherheit UND der Geschäftskontinuität

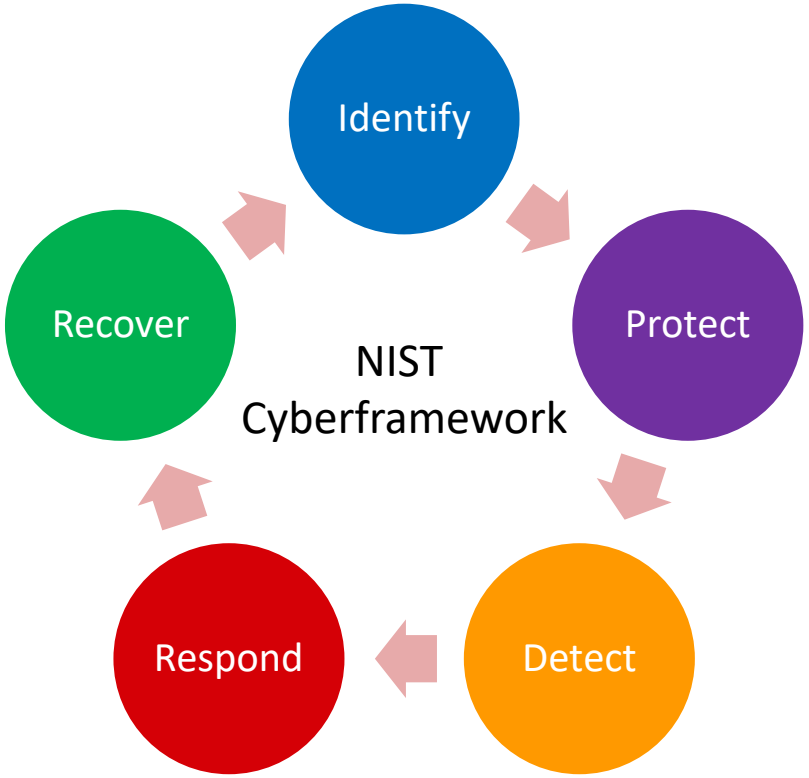
- Ein widerstandsfähiges Unternehmen...
  - verwendet einen ganzheitlichen Ansatz, um die Arbeit zu verstehen/priorisieren und das Risikomanagement in die täglichen Abläufe in ALLEN Geschäftsbereichen zu integrieren
  - weiss, welche Informations- und Kommunikationssysteme unternehmenskritisch sind, und hat Massnahmen ergriffen, um Incidents zu verhindern

- ABER ... Trotz aller Bemühungen wird es zu Cyber Security-Vorfällen kommen!

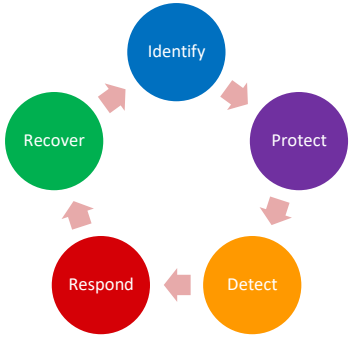
Von der Abwehr hin zur Cyberresilienz

Weg vom. Reinen Fokus auf präventive (meist technische) Schutzmassnahmen

Hin zur verbesserter Detektion und Reaktion



Setzen Sie Grundmassnahmen rigoros um



Zuweisen von Aufgaben, Kompetenzen Verantworlichkeiten

Kennen der unternehmenskritischen Daten und Geschäftsprozesse

Inventar der IT-Systeme und Software (auch IoT)

Risikomanagemnt

Durchsetzen von Sicherheitsmassnahmen bei der Zusammenarbeit mit Dritten

Systemhärtung und Vulnerability-Mngt

Sensibilisierung Und Training

Identitäts- und Zugriffsmanagement, inklusive Aufzeichnungen

Regelmässiges „Patching“ aller IT-Systeme

Anti-Malware Erkennung

Segmentierung und Überwachung des Netzwerkes

Periodische/ kontinuierliche technische Sicherheitstests (auch in der Entwicklung)

Entwickeln und Testen/ Üben der Cyber-Notfallpläne

Security Incident Response Pprozess

Back-up(inklusive Malwareschutz)

Massnahmen nach einem erfolgreichen Angriff

- Im Falle einer Infektion empfehlen wir den Computer sofort von allen Netzwerken zu trennen.
- Danach Neuinstallation des Systems und Ändern aller Passwörter.
- Danach können die Backup-Daten wieder zurückgespielt werden.
- Wenn kein Backup der Daten vorliegt, die verschlüsselten Daten behalten und sichern, damit Sie sie allenfalls später noch entschlüsseln können, sollte hierzu eine Lösung gefunden werden.
- In jedem Falle den Vorfall der Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) zur Kenntnis zu bringen und
- Anzeige bei der lokalen Polizeidienststelle zu erstatten.
- Verzichten Sie darauf, ein Lösegeld zu bezahlen. Es gibt es keine Garantie die Schlüssel für die Entschlüsselung zu bekommen

Ich wurde Opfer eines Angriffs - Wie komme ich wieder auf die Füsse?

- Erkennen (Log Files, ohne SIEM Werkzeuge zum Korrelieren sehr aufwendig)
- Sofortmassnahmen
  - Datensicherheit gewährleisten
    - Backups offline nehmen (Am 17.10 – 21:00)
    - Betroffene Computer sofort vom Netzwerk entfernen (Ab 17.10 – 21:00)
  - Lieferanten zur Unterstützung aufbieten
    - Weitere Manpower wird benötigt
    - Security Spezialisten werden benötigt
  - Beziehungen bei Lieferanten und Partner nutzen

- Verstehen / Klassifizieren
  - Welche Schadsoftware wurde eingefangen?
    - Wie hoch ist das Schadenspotenzial der eingefangenen Schadsoftware?
    - Auf welchen Kanälen verbreitet sich die Schadenssoftware?
    - Wie weit ist hat sich die Schadsoftware schon verbreitet?
    - Handelt es sich um einen mehrstufigen Angriff?
      - In welcher Stufe befinden wir uns?
    - • Welche Mittel und Tools sind für die Eingrenzung notwendig?

Ich wurde Opfer eines Angriffs - Wie komme ich wieder auf die Füsse?

- Bekämpfen (mit externen Spezialisten)
  - Verteidigung
    - Diverse Tools zur Erkennung von Schadsoftware und suspektem Verhalten
    - Korrelation von diversen Quellen
  - Ausserbetriebnahme einzelner Systeme
  - Angriff – Säuberung
    - Datenkorrelationswerkzeuge implementieren, Automatische Korrelation diverser Systeme
    - Fullscan auf sämtlichen Systemen
      - Sämtliche infizierte Systeme säubern / besser neu installieren
      - Infizierte Userprofiele neu anlegen

Informationsquellen und Hilfsmittel

- IKT-Minimalstandard: Minimalstandard zur Verbesserung der IKT-Resilienz
  - https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html
- NIST Cybersecurity Framework Core
- NIST Guide to Industrial Control Systems (ICS) Security
- ISO 2700x
- COBIT Control Objectives for Information and related Technology (COBIT)
- Bundesamt für Sicherheit in der Informationstechnik (Deutschland), BSI 100-2.