OST
Eastern Switzerland
University of Applied Sciences

Incident Response Summary

Zusammenfassung

Studiengang Informatik
OST - Ostschweizer Fachhochschule
Campus Rapperswil-Jona

Frühjahrssemester 2022

Autor:	legenda.gr
Version:	21. Juni 2022
Dozent:	Gregor Wegberg

Inhaltsverzeichnis

1 Incident Response Grundlagen

1.1 Definition

Incident Response are actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it.

- Incident Response ist die Aktivität einen Informationssicherheitsvorfall zu behandeln
- Ein Vorfall ist ein oder mehrere Informationssicherheitsereignisse, die (wahrscheinlich) zu einem Schaden für die Organisation führen
- Ein Ereignis verletzt die Aktivitäten eines Unternehmens zur Sicherstellung der Informationssicherheit
  - nicht nur FW deaktivieren etc. → MA, welcher NB entsperrt liegen lässt kann auch ein Security Incident werden
- Incident Response ist die Bewältigung einer Verletzung der Informationssicherheit

1.2 Information Security Incident (Informationssicherheitsvorfall)

Einzelnes oder eine Reihe von ungewollten oder unerwarteten Informationssicherheitsereignissen, die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten zu gefährden und die Informationssicherheit zu bedrohen.

1.3 Information Security Event (Informationssicherheitserreignis)

Erkanntes Auftreten eines Zustands eines Systems, Dienstes oder Netzwerks, der eine mögliche Verletzung der Politik oder die Unwirksamkeit von Maßnahmen oder eine vorher nicht bekannte Situation, die sicherheitsrelevant sein kann, anzeigt.
Bei einem **Ereignis** kann etwas vorhanden sein (z.B. AV Meldung → true positive oder falscher Alarm?) → falls Mimikatz in AV Report steht → befindet man sich schon im **Event** und nicht mehr im **Ereignis**
Bei einem **Event** ist wirklich etwas (effektiver Security Vorfall)!.

1.4 Ziel Informationssicherheit

CIA Triad → Confidentiality, Integrity, Availability

1.4.1 Confidentiality

Information wird unbefugten nicht verfügbar gemacht oder offengelegt.

1.4.2 Integrity

Information ist richtig und vollständig.

1.4.3 Availability

Information ist für eine befugte Entität bei Bedarf zugänglich.

1.5 Schützenswerte Daten

- Kundendaten → DSG (Datenschutz Gesetz)/ GDPR
- Mitarbeiterdaten → DSG
- PII/ PHI → DSG
- Backups
- Trade Secrets

2 Aktuelle Bedrohungslage

2.1 Vishing

Beim Vishing (Voice Phishing) werden Personen mündlich zu Handlungen aufgefordert, von denen sie glauben, sie seien in ihrem Interesse. Vishing setzt oft da an, wo Phishing an seine Grenzen stößt.

2.2 Vishing + E-Mail Phishing

Oft fängt das ganze mit Phishing (z.B. via E-Mail) an und es weitet sich schlussendlich ins Vishing aus.

Beispiel:
Jemand besucht eine Social-Media-Plattform, klickt auf einen verlockenden Link – und schon erscheint ein blauer Bildschirm mit einer Warnmeldung und der Aufforderung, bei der angezeigten gebührenfreien Telefonnummer anzurufen, um ein ernsthaftes Problem mit dem Computer zu beheben.
Am Telefon meldet sich ein freundlicher Techniker, der gerne bereit ist zu helfen – allerdings nur gegen Bezahlung. Nachdem für den Kauf der Software, mit der das Computerproblem behoben werden soll, die Kreditkartendaten zur Verfügung gestellt wurden, ist der Betrug komplett und kommt das Opfer teuer zu stehen.
Die Software funktioniert nicht, und vom hilfsbereiten Techniker wird man nie wieder etwas hören. Der Benutzer ist ein weiteres Opfer der als „Vishing“ bezeichneten Betrugsmethode geworden.

2.3 Mögliche Folgen

- eBanking Trojaner wird installiert
- Zukünftige eBanking-Aktivitäten können durch die Cyberkriminellen manipuliert werden
  - Betrag ändern, Zielkonto ändern, SMS-Verifikation wird ausgehebelt
- Aktuelle Antivirussoftware konnte die Schadsoftware nicht identifizieren
- Hätte jede andere Schadsoftwareart sein können!

2.4 Ransomware

How Ransomware works!

2.4.1 Ransomware Angriffe

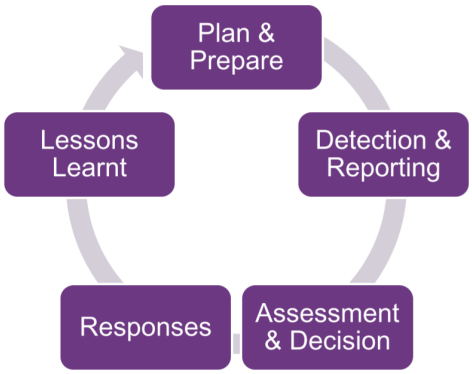
1. Kompromittierung
2. Sensible Daten entwenden
3. Daten verschlüsseln (1. Erpressung)
4. Mit Veröffentlichung der Daten drohen (2. Erpressung)
5. Optional: Öffentlich an den Pranger stellen
6. Optional: Mit DDoS drohen (3. Erpressung)
7. Assoziierten Personen drohen (4. Erpressung)
8. Optional: Business E-Mail Compromise (BEC), Phishing etc.
9. Optional: Veröffentlichung der gestohlenen Daten

2.5 Wie schützen wir uns

- Mehrere, nacheinander gelagerte Schutzmechanismen (Defense in depth)
- Vertrauen nicht einem einzigen Produkt und Mechanismus (z.B. AV-SW, FW)
- 100% Sicherheit gibt es nicht, aber:
  - Wir können die Kosten für Angreifer erhöhen
  - Wir können Angreifer verlangsamen
  - Wir können Angreifer erkennen
  - darum gibt es Incident Response

3 Incident Response Prozess

3.1 ISO/IEC 27035-1



3.1.1 Plan & Prepare

- Organisatorischen Incident Management Rahmen schaffen
- CEO/ Geschäftsführer muss vollstes commitment für Cyber Security zeigen
- Incident Management Plan festlegen
- Incident Response Team (IRT) etablieren
- Klassifikation festlegen, Formulare erstellen
  - Damit im Notfall nicht wichtige Angaben im Formular vergessen gehen (z.B. SN Festplatte)
- Intern & extern vernetzen, vor allem verantwortliche Entitäten für Informationssicherheitsereignisse, -vorfälle & Schwachstellenmanagement
  - Connection/ Beziehungen aufbauen um im Notfall Zeit zu sparen
- Trainieren, schulen, simulieren und Bewusstsein steigern (Red Teaming etc.)
- Fähigkeiten / Maturität überwachen

Ukraine Konflikt aus IR Sicht

- Heute die Projekte starten (jetzt ist Unterstützung GL sehr hoch)
- Geoblocking einschalten (auf FW)
- Logs beobachten/ Monitoring
- Low hanging fruits
- Awareness Kampagne
- Notfallkontakte überprüfen
- Tabletop Übungen
- Genauer Ablauf sollte eine Organisation selber entwickeln (Incident Management Plan)
- Diverse Quellen können ein Ereignis feststellen und/oder melden (SIEM, FW, SOAR, EDR, etc.)
- **Wichtig**:
  - Meldewege sind definiert
  - Meldewege sind allen relevanten Parteien bekannt (Notfallnummernblatt)
  - Empfänger der Meldung wissen, was damit zu tun ist

  - Bei Meldequelle bedanken, Resultat/Folge der Meldung teilen → Meldungen motivieren!

- IT-Sicherheitssysteme (technische Quellen)
  - Proaktive Detektion vs. Reaktive Detektion
  - Protokolle, SIEM, Schwachstellen-Scanner
  - Deception Technologie, z. B. Honeypots, Honeytokens, Honey Accounts etc.
    * Testen, ob Unternehmen Informationen weiterverkauft
    * *Honeypod* wird eine Einrichtung bezeichnet, die einen Angreifer oder Feind vom eigentlichen Ziel ablenken soll oder in einen Bereich hineinziehen soll, der ihn sonst nicht interessiert hätte (z.B. in Form eines Scheinziels).
  - Email Traps (Spamtrap), Sandbox
- Wenn technische Quellen vorhanden sind und genutzt werden: Merkt jemand die Meldung?
  - Automatisierung, unübersehbarer Alarm, SIEM (Aspekte der Cyber Defense)
- Organisation
  - Interne Partner: IT-Betrieb, Netzwerkbetrieb, IT Support
  - externe Partner
    * ISP, MSP (Managed Service Provider), IT-Dienstleister, Security-Partner, etc.
      · Mit Dienstleistern Kommunikationspflicht festlegen
    * Cloud Dienstleister (SaaS, IaaS, PaaS, ...) → Schattendienstleister
      · Security-Kontakt einrichten
    * IT-Security-Partner, nationales CSIRT / NCSC
    * Offene und geschlossene Gemeinschaften zum Informationsaustausch
  - Kommunikation im Vorfeld definieren!
  - Medien
    * Kann das Incident Response Team damit umgehen?
    * Nein! Wenn Medien involviert sind:
      · Public Relations, Marketing, Presseabteilung, ... involvieren
      · Geschäftsleitung sollte im Normalfall informiert werden
- Mitarbeiter
  - Wissen diese wo sie sich melden dürfen?
  - Sind sie motiviert sich zu melden?
- Externe Individuen
  - White/Gray/Black Hats, Sicherheitsforscher, Bug Bounty usw.
  - Have I Been Pwned, "Darknet Monitoring/ "Cyber Threat Intelligence"
- Weiss der Empfänger/die Empfängerin, was mit einer Meldung zu tun ist?

Reporting

- **Ziel**: Wer, was, wo und wann für die weitere Verarbeitung festhalten.
  - Wer hat es entdeckt? Wie erreichen wir diese Person?
  - Was wurde wann beobachtet? Wo wurde es beobachtet?
  - Wann wurde was bereits gemacht?
- Je nach Organisation, Quelle und Auftrag diverse Formate denkbar:
  - Mündlich am Telefon oder in Person
  - Schriftliches oder digitales, vordefiniertes Formular

3.1.2 Assessment & Decision

- **Ziel**: Feststellen, ob das Ereignis ein Vorfall ist
- Informationen zum Ereignis sammeln
- Entscheidung basierend auf Informationen:
  - Kann es ein Vorfall sein? → Eskalation zum IRT (Incident Response Team)
  - Ist es ein Vorfall? → IRT startet Response-Phase
  - Ist es falschpositive Meldung? → Falschpositivenrate im Lessons Learnt senken
- Wichtig: Spätestens ab hier detailliertes Protokollieren
  - Was wurde wann, wo und von wem festgestellt?
  - Welche Folgen hatte es?

3.1.3 Responses

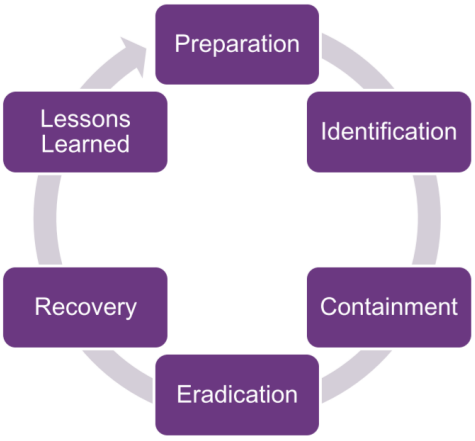
- **Ziel**: Vorfall bewältigen/lösen
- Die Einschätzung (Klassifikation, Schweregrad etc.) fortlaufend neu bewerten
- Alle beteiligten Personen führen detailliertes Protokoll
- Beweise sammeln und sichern für eine mögliche spätere Untersuchung

3.1.4 Lessons Learnt

Lessons Learnt geht oft vergessen, ist aber sehr wichtig dass nicht wiederholt die gleichen Fehler gemacht werden.

- Aus dem geschehenen lernen, analog einer Retrospektive oder einem Post Mortem
  - Welche Schutzmassnahmen anpassen/verbessern?
  - Wie können wir das Incident Management verbessern?
  - Müssen wir unser Risikomanagement anpassen/ergänzen?
- **Wird sehr gerne übersprungen / ignoriert**
- Absolut essenziell zur Steigerung der IT-Sicherheit und Reaktion auf Ereignisse/Vorfälle

3.2 SANS Incident Response Prozess



3.2.1 Preparation

- Richtlinien, Prinzipien, Regeln etc. festlegen
- Prozess und Vorgehen für Vorfallbewältigung definieren
- Kommunikationsplan: intern, extern, Partner etc.
- Computer Incident Response Team (CIRT) definieren
- Notwendige Werkzeuge bereitstellen
- Trainieren
- **Ziel**: Technische und organisatorische Rahmenbedingungen vorbereiten/pflegen

3.2.2 Identification

- Beginnt mit der Meldung eines möglichen Ereignisses
- Entscheiden, ob ein Ereignis vorliegt
- Prüfen, ob es ein Vorfall ist
- Spätestens in dieser Phase muss alles dokumentiert werden: Wer, was, wo, weshalb und wie

3.2.3 Containment

- **Ziel**: Schaden mindern und weiteren verhindern
  1. Kurzfristiges Containment: so früh wie möglich Schaden eingrenzen
  2. System Back-Up: Bevor Systeme zurückgesetzt werden diese forensisch sichern
  3. Langzeit Containment: Temporäre Massnahmen, bis Eradication abgeschlossen ist

Beispiel Containment

- Domain sperren
  - Soll `p.estonine.com` oder `estonine.com` gesperrt werden?
- IP-Adresse vom DNS Resource Record A (IPv4) und AAAA (IPv6) sperren
- In DNS Logs nach Domain suchen
  - Domain ist ein Indicator of Compromise (IOC)!
- In Firewall, Forward Proxy etc. Logs nach IP-Adresse suchen

  - IP-Adresse ist ein IOC!

- *Scheduled Task* ist ein starker *Indicator of Compromise (IOC)*
  - Wird von Schadsoftware erstellt & Name ist oft fest in Schadsoftware einprogrammiert
  - Können mit PowerShell, WMI etc. nach Scheduled Tasks mit diesem Namen auf allen Windows-Systemen suchen

3.2.4 Eradication

- Schädliches und unerwünschtes entfernen
- Betroffene Systeme wiederherstellen ($\neq$ Backup wiederherstellen, zumindest nicht immer)
- System wieder in sauberen Zustand bringen (Malware entfernen, etc.)

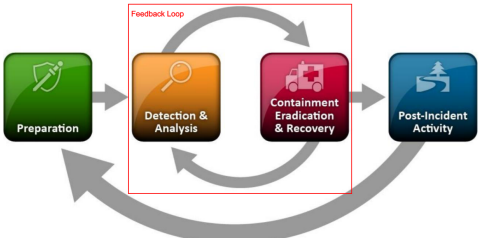
3.2.5 Recovery

- Betroffene Systeme wieder in den Betrieb bringen
- Vorsicht! Sollte nicht erneut zum Vorfall führen
  - System überprüfen & überwachen
- Typische Herausforderung: Wann ist ein System *sauber*?

3.2.6 Lessons Learned

Siehe 3.1.4

3.3 NIST Incident Response LifeCycle



NIST Standard mehr technisch, ISO Standard mehr fürs Management