H. Übungen

Überblick über Übungen

was erwartet uns in der Praxis? und in der Klausur?

- wir bereiten eine Cyberversicherung vor…
- eine „frische“ IT-Infrastruktur entsteht
  - Konzeption (Sicherheit) / Schutzvorkehrungen / sonst
- eine „alte“ IT-Infrastruktur wird übernommen und ist zu optimieren
  - untersuchen / Änderungsbedarf ermitteln (Sicherheit) / Schutzvorkehrungen treffen / sonst
- wie verhalte ich mich gegenüber einem Vorfall?
  - Ransomware-Angriff
  - erschwindelte Überweisung

H.1. Übung 1

„Erschwindelte Überweisung“

1. Welche Folgen hat der Zwischenfall?
2. Warum war der Angriff möglich?
3. Welche Maßnahmen würden diesen Vorfall verhindern?
4. Welche Maßnahmen würden die Folgen abmildern?
5. Was hätte K im Vorfeld unternehmen müssen?
6. Wie ist hier im Einzelnen vorzugehen (nachdem es zum Zwischenfall gekommen ist)?

<u>Achtung</u>: nicht nur direkte Folgen des Vorfalls (Überweisung) sind zu betrachten (siehe insbesondere: kompromittierte Infrastruktur!)

H.1. Übung 1 - Erschwindelte Überweisung

1. Welche Folgen hat der Angriff?

(nicht die Beträge - nur einzelne Posten und Probleme)

- das überwiesene Geld
- Betriebsunterbrechung / -störung (falls es dazu kommt)
- Untersuchung / Forensik (zwingend!) und ihre Kosten
  - externe Experten
  - eigenes Personal
- Austausch / Reparatur von Hardware / Software
- vorläufige Absicherung / vorläufiger Betrieb
- Vertragsstrafen, Haftung für Schäden und Bußgelder

**auch wenn nicht auf den Zwischenfall zurückzuführen:
Optimierung des Systems ist vorzunehmen!**

H.1. Übung 1 - Erschwindelte Überweisung

2. Warum war der Angriff möglich?

- Posting => Instagram / Tweet
- gefälschte E-Mail nicht erkannt
- gefälschte und schädliche Webseite aufgerufen
- Arbeitsrechner ermöglichten Installation der Schadsoftware
- IT des Unternehmens hat Angriffe nicht erkannt / abgewehrt
- den darauffolgenden - gefälschten - Anweisungen gefolgt

insgesamt eine lange Kette von Ursachen, von denen viele kumulativ benötigt werden, den schädlichen Angriff erfolgreich durchzuführen

H.1. Übung 1 - Erschwindelte Überweisung

3./4./5. Angriff verhindern / Folgen abmildern?

- **Lücken** schließen / **Systeme abhärten / besser schützen**
- Redundanzen herstellen (gespiegelte IKT?) / **Backup**!
  - Business-Continuity-Management etablieren (**Recovery**!)
- Robustheit der **Sicherheitskonzepte** prüfen
- IT-Trainings (sichere Bedienung, „Awareness“, IT-Kompetenz)
- Krisenmanagement etablieren

manche Maßnahmen helfen sowohl bei Vermeidung eines Angriffs wie auch bei Abmilderung seiner Folgen

H.1. Übung 1 - Erschwindelte Überweisung

6. Wie ist hier im Einzelnen vorzugehen?

das Szenario erfordert mehr, als nur die Abschreibung des gezahlten Geldes!

- Prio A: was genau ist passiert? Forensik!
- Entscheidung treffen - was ist wichtiger:
  - Betrieb beibehalten
  - sichern und alles stoppen
- Kategorie 1: Organisation
- Kategorie 2: Technik

Oberste Prämisse: Ruhe bewahren und besonders sorgfältig vorgehen - nur überlegtes Handeln kann zur Schadensbegrenzung beitragen

H.2. Übung 2 - Ransomware-Angriff

Krisenmanagement - Organisation

- systematisch Vorgehen
- Personen, die in der Lage sind, Problem zu verstehen, als Team einsetzen
- Einteilung: Tagesgeschäft <=> Schadensbekämpfung
- Meldepflichten?
- Externe Berater einholen
- Reservetechnik identifizieren (andere Standorte? vor Kurzem ersetzte Systeme?)

Auch hier gilt: Ruhe bewahren und vorsichtig, sorgfältig vorgehen!

H.2. Übung 2 - Ransomware-Angriff

Krisenmanagement - Technik

- (potenziell) infizierte Systeme niemals mit Admin-Rechten inspizieren!
- infizierte Systeme isolieren (Netzwerk, Datenträger)
- Angriff identifizieren
- Systeme komplett neu aufsetzen
- mehrfach Zugangsdaten ändern / zurücksetzen
- Netzwerkanalyse / Virenscans
- Backups inspizieren (!)
- Netzwerkstruktur eventuell neu aufbauen (Active Directory)

Auch hier gilt: Ruhe bewahren und vorsichtig, sorgfältig vorgehen!

H.3. Übung 3 - Cyber-Versicherung / Audit

Was ist zu tun?

- Sicherheitsprozess ist zu implementieren (PDCA)
- die dabei notwendigen Analysen sind durchzuführen:
  - (relevante) Systemeigenschaften erfassen
  - Schutzbedarf ermitteln
  - Bedrohungen erfassen
  - Sicherheitsarchitektur schaffen

dokumentieren!

- einzelne Maßnahmen in allen Bereichen ergreifen:
  - Verträge + Organisation + Personal + Infrastruktur + Technik

zu technischen Maßnahmen bitte vertiefen

H.3. Übung 3 - Cyber-Versicherung / Audit

Was ist zu tun? => technische Maßnahmen

(siehe Gliederung / Präsentation => G. 2. c.)

- Sicherungskopien + Redundanz der Infrastruktur
- Vermeidung von Sicherheitslücken
  - wer ist für Einspielung von Updates verantwortlich?
- Netzwerk absichern - Router, Firewall korrekt konfiguriert?
- Vertraulichkeit, Verschlüsselung, VPN
- Analyse + Überwachung
- bei Bedarf: Isolation (Virtualisierung?)
- etc.

Ende!

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?