Zwei Jahre nach dem Vorfall – ein Erfahrungsbericht

21.03.2025

Thomas Wallutis

Agenda

Zur Person

- Thomas Wallutis
- Externer Informationssicherheitsbeauftragter der IHK-GfI GmbH
- Beteiligt am Wiederaufbau
- Mitarbeiter der @-yet GmbH
  - Forensik im Rahmen des Vorfalls
  - Wiederaufbau im Rahmen des Vorfalls
- Weitere Informationen zur @-yet GmbH gerne in der Pause

Ausgangssituation

Die IHK-Welt

- IHK-Organisation: 79 IHKn, DIHK, >200 Standorte, >8.000 User, >20.000 IP´s
- Kerngeschäft: hoheitliche Aufgaben, Bildung, Beratung, Interessenvertretung
- IHK GfI ist als Managed Service und Cloud Provider mit rd. 340 FTE der zentrale IT- Dienstleister der IHKs:
  - Leistungsspektrum ca. 240 IT-Services (ERP, diverse Web- und Fach-Applikationen, eUZ, IP-Telefonie, Mail, etc.) sowie WAN und zentraler Internetzugang
  - IHK-GfI betreibt ein CERT (Computer Emergency Response Team)

Die IHK-Welt

- Komplexe Systemlandschaft inklusive Eigenentwicklungen
- Zentrale und dezentrale IT
- Basis-Sicherheitsvorgaben
  - Vorgaben, Verbote und Empfehlungen
  - Verbindlich für die IHK-GfI und die Kammern

Der Angriff

Die Mail, die man nie bekommen will

Von: [redacted]
Gesendet: Mittwoch, 3. August 2022 11:37
[redacted]
Betreff: Sicherheitsvorfall - Verdacht [redacted] Account Kompromittierung und Missbrauch!!
Priorität: Hoch

Hallo zusammen,

heute vormittag wurde eine verdächtige Aktion mit einem [redacted] Konto [redacted] bemerkt.
Eine weitergehende Analyse hat bestätigt, dass diese Aktion von einem kompromittierten Account durchgeführt wurde!

Der Zugriff geschieht durch eine Kundennetzwerk, welche die GfI im RZ hostet.

Wir sind mit allen Fachteams in der Behandlung des Vorfalls.
Der Umfang kann zur Zeit noch nicht abgeschätzt werden

Was wir wissen

- Entdeckt wurden die Angreifer am 03.08.2022
- Begonnen hat der Angriff (vermutlich) am 19.05.2022
  - Frühere Spuren konnten nicht identifiziert werden
  - Scanning von Systemen
- Erste erfolgreiche Aktion am 24.05.2022
  - Details können an dieser Stelle nicht gegeben werden
- Angreifer hinterließen nur wenige Spuren
  - Eher APT als Ransomware

Was wir nicht wissen

- Wer waren die Angreifer?
- Was war das Ziel?

Attribution ist schwer. Und Spekulationen sind nicht zielführend.

Meldungen im Web

Top stories

Mögliche Cyberattacke auf IHK

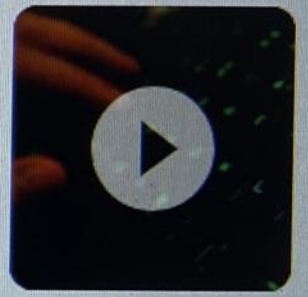
t-n digital pioneers

IHK von massivem Cyber-Angriff getroffen

7 hours ago

Bayerischer Rundfunk

Cyber-Angriff auf die IHK – auch die IHK Mainfranken betroffen



1 hour ago

WDR

Möglicher Hackerangriff: IHK–Systeme abgeschaltet - Ruhrgebiet - Nachrichten

3 hours ago

CHIP

Wegen geplanter Cyberattacke: Industrie- und Handelskammern...

4 hours ago

Forensik

Forensik

- Forensische Untersuchung durch die @-yet GmbH
  - Beim BSI gelisteter APT Response Dienstleister
  - Großes Forensik-Team
  - Mehrere hundert Fälle in den letzten sechs Jahren
- Analyse durch mehrere Forensiker (im Durchschnitt 5)
  - Dauer 2 Monate
- Erstellung eines umfangreichen Berichtes
- Bericht wurde durch eine externe Stelle begutachtet

Die Auswirkungen

Auswirkungen

- Keine Verschlüsselung von Daten oder Systemen und, soweit erkennbar, kein Ausleiten personenbezogener Daten
- Massive Auswirkungen auf Mitarbeitende
  - Man muss die Belastbarkeit der Mitarbeitenden im Auge haben!
- Kunden sind in der Arbeitsfähigkeit stark beeinträchtigt worden
- Wiederanlauf hat Zeit gekostet, da alle Systeme gescannt und gehärtet wurden
  - Rechnen Sie in Monaten, nicht in Wochen!

Auswirkungen

Nur wenige Betroffene gehen aufgrund der Lösegeldzahlung pleite. Firmen scheitern am Produktionsausfall oder am Wiederaufbau.

Mikko Hypponen, Keynote BruCon 2023 (https://www.youtube.com/watch?v=3194_DjIf_A)

Wiederaufbau

… und nun ?

Ruhe bewahren !

Systematisch vorgehen !!

Notfall-Leitlinie/ Krisenstab !!!

Notfall-Leitlinie - Komponenten (Auszug)

gem. BSI Standard 200-4

Krisenstab

GF
CERT, IT-SB, DSB
Technik
Ressourcen

Schadensanalyse

Was ist passiert?
Was wissen wir?

Sofortmaßnahmen

Sicherungen und Logs sichern!
Folgeschäden verhindern!
Was tun wir als nächstes?

Kommunikation

Aufsichtsrat
Kunden (HGFs & IT-Ltr.)
Mitarbeiter

Meldepflichten

Datenschutz
Polizei
(BSI)

Externe Unterstützung

Spezialisten hinzuziehen:
- APT-Response-Dienstleister
- Agentur für Krisenkommunikation

Dokumentation

Aktivitäten protokollieren

Entscheidungsregister

Entscheidungen dokumentieren

Sofortmaßnahmen

- Kappen der Internetverbindung
- Aufbau einer alternativen Kommunikationsinfrastruktur
- Einberufen eines Wiederaufbau-Teams
  - Geschäftsführung
  - Leiter der Fachabteilungen
  - CERT + Security-Manager
  - Externe Unterstützung durch @-yet (Thomas Wallutis)
- Anwenden der Notfall-Leitlinie

Vorgehensweise

- Grundannahme: keine Manipulation von Firmware
  - Z.B. Switches nach Zurücksetzen auf Werkseinstellung weiter verwendbar
- Alle anderen Systeme galten als potentiell kompromittiert
- Neuinstallation war der bevorzugte Weg
- Falls nicht möglich: gründliche Überprüfung
  - User, Gruppen, geplante Tasks, Cron Jobs etc.
  - Commits wurden manuell geprüft

Vorgehensweise

- Maßnahmen durchliefen ein mehrstufiges Verfahren
  - Einreichung
  - Vorstellung im Meeting
  - Bewertung durch CERT/INFOSEC und @-yet bzgl. Restrisiko
  - Freigabe durch GF
- Netzwerkunterteilung
  - Rotes Netz
  - Grünes Netz
  - „Grüne Inseln im roten Meer“

Vorgehensweise

- Datenprüfung mit Hilfe einer Datenschleuse
  - Virenscanner und weitere Tools
  - Einordnung in ROT (verdächtig), GRÜN (unverdächtig) und GRAU (muss manuell geprüft werden
- Systemüberprüfung
  - Schwachstellenscanner
  - IoC-Scanner

Vorgehensweise

- Umbau der vorhandenen Umgebung
  - Stärkere Segmentierung
  - Nutzung von Host-based Firewalls für eingehenden Traffic
    - Siehe BSI GS „SYS.1.1.A19 Einrichtung lokaler Paketfilter (S)“
  - Umbau der Authentifizierungs-Infrastruktur

Probleme

- Ungewohnte Situation
- Hoher Druck
- Remote arbeiten notwendig
  - Technische Voraussetzungen
- Die gewohnte technische Umgebung steht nicht zur Verfügung

Probleme

- Ist die notwendige Dokumentation vorhanden?
- Sind die erforderlichen Personen vorhanden?
  - Single Point of Knowledge
- Abgleich neue Ideen mit gewohnten Abläufen
  - Technisch (z.B. Netzwerksegmentierung)
  - Organisatorisch (z.B. Administration)

Das Ziel ist eine Umgebung, in der man einzelne Teile „kontrolliert abbrennen“ lassen kann.

Lessons learned

Lessons learned

- Man kann sich immer verbessern
  - Organisatorisch
  - Technisch
- Vorhandene Maßnahmen wurden geprüft und ggf. erweitert
- Es wurde ein umfangreiches IT Security Programm mit über 30 Teilprogrammen eingerichtet
  - Business Continuity Management
  - Ausweitung des (zertifizierten) ISMS

Lessons learned

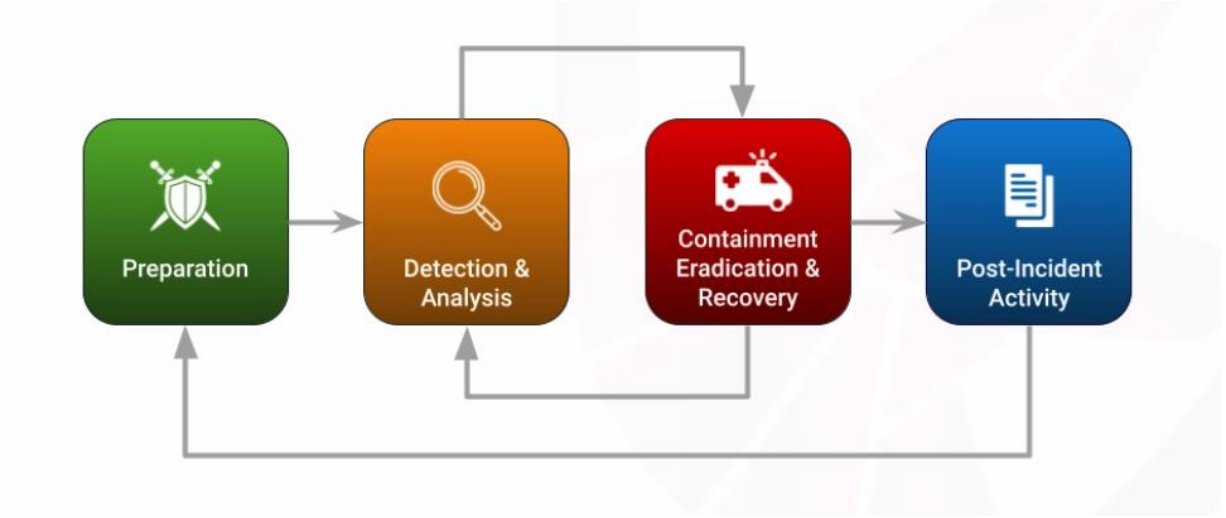
- Awareness
- Weiterbildung
- Aufstockung des Security Teams
- Notfallübungen
  - Technisch
  - Table Top

Lessons learned

- Kundenkommunikation
  - Was kann/soll/muss gesagt werden?
  - Über welches Medium?
- Kommunikation mit Mitarbeitenden
  - Beruhigen
  - Kommunikation steuern
- Kommunikation nach außen
  - Wer spricht mit wem über welche Inhalte?

Programm New IT Security

- Drei Säulen
  - Sicherheit erhöhen
    - Z.B. Privileged Access Management
    - Z.B. Vulnerability Scanning (erweitert)
  - Erkennung verbessern
    - Z.B. Ausbau Logging
    - Ressourcenausbau
  - Resilienz steigern
    - Z.B. Awareness Training (erweitert)



- Flankiert von Governance/Compliance
  - Z.B. BSI Grundschutz

Fazit

Fazit

- Eine Cyber-Attacke im Leben reicht
  - Aber ist der Wunsch realistisch?
- Eine gute Vorbereitung ist wichtig
- Klare Strukturen und Vorgehensweisen
- Es gibt immer was zu verbessern
- Informationssicherheit ist ein Prozess, kein Projekt
- Informationssicherheit ist mehr als Technik

- Wir waren gut. Jetzt sind wir besser.

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!