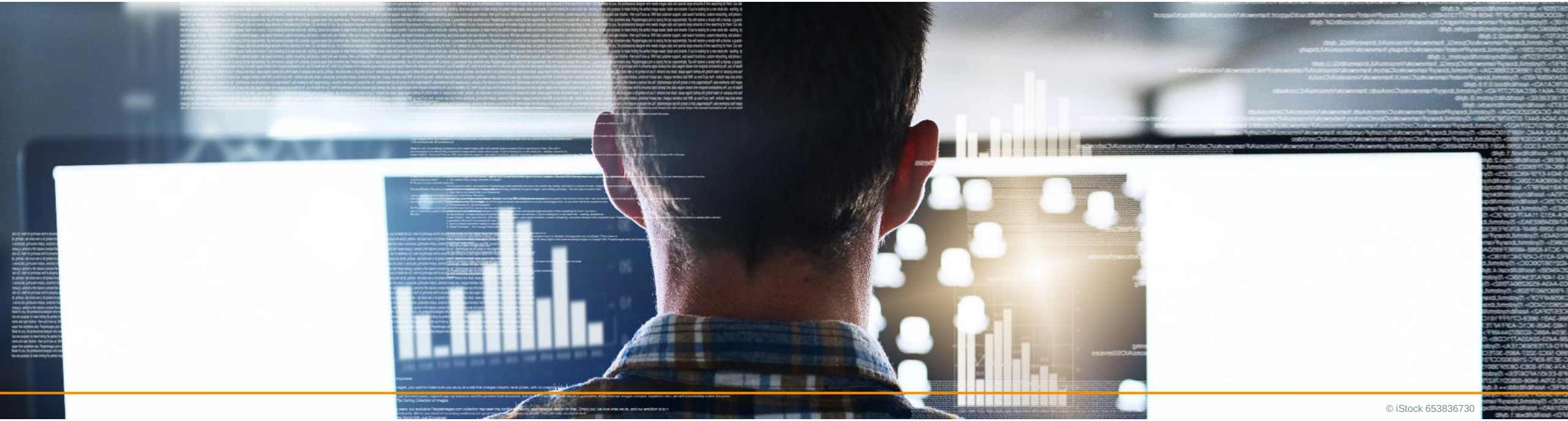


© iStock 653836730

Cyber Defence Lifecycle:
Der Weg zurück in den Normalbetrieb

SEC Consult
an atos company

SEC Consult
an atos company

Dipl.-Ing. Fabian Mittermair

Managing Director

E-Mail: f.mittermair@sec-consult.com

SEC Consult Unternehmensberatung GmbH
Leopold-Ungar-Platz 2, 1190 Wien

www.sec-consult.com

What we do?

Offensive Security

Information Security Consulting

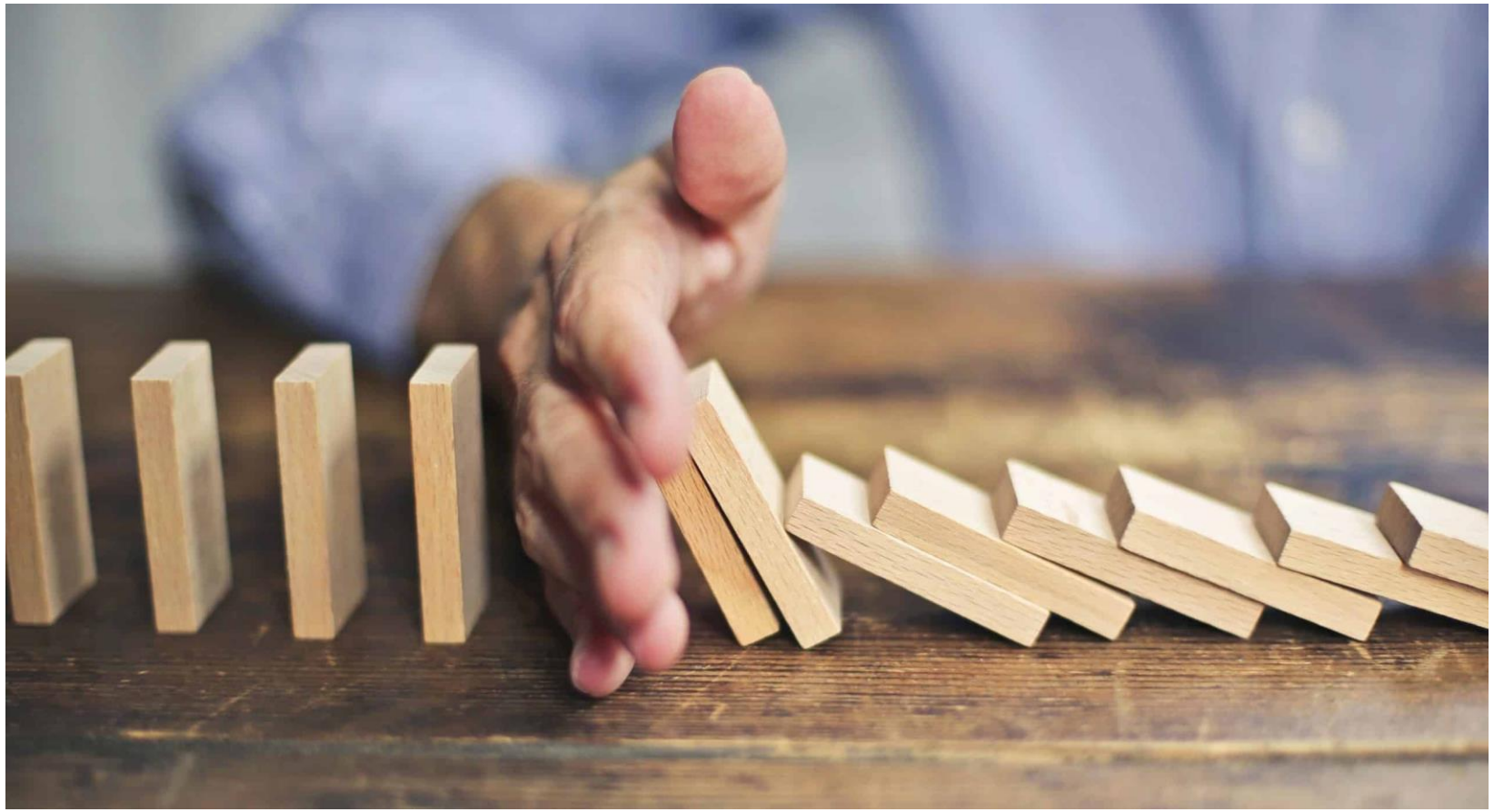
Incident Response

SEC Consult
an atos company

Incident …

SEC Consult
an atos company

Incident Response



Beispiel: Kryptolocker

Ich brauche meine Daten zurück!

Beispiel: Kryptolocker

Beispiel: Kryptolocker

It‘s not personal, Sonny.
It‘s strictly business

Incident Response Lifecycle

Incident response is a structured process organizations use to identify and deal with cybersecurity incidents. Response includes several stages, including preparation for incidents, detection and analysis of a security incident, containment, eradication, and full recovery, and post-incident analysis and learning.

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

SEC Consult & Atos führen Sie durch den gesamten Incident Response lifecycle

SEC Consult
an atos company

Umfangreiches Offensive Security Portfolio

Penetration Testing

Mobile Security

SAP Security

Infrastruktur Security

IoT Security

Red Teaming

Bundesamt für Sicherheit in der Informationstechnik
Anerkannte Prüfstelle für IT-Sicherheit

Atos

Managed SOC/SIEM

SIEM Implementierung & Betrieb

SIEM as a Service

SOC as a Service

Managed Incident/Event Handling

Allianz für Cyber-Sicherheit
Partner

SEC Defence Taskforce Preparation

Incident Operation
Handbook & **Checklisten**

Incidend Readyness
Maturity Assessment

War Games und
Krisenübungen

Red Team vs. Blue Team
(Purple Team Trainings)

SEC Consult
an atos company

Incident Response Lifecycle

Incident response is a structured process organizations use to identify and deal with cybersecurity incidents. Response includes several stages, including preparation for incidents, detection and analysis of a security incident, containment, eradication, and full recovery, and post-incident analysis and learning.

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

SEC Consult & Atos führen Sie durch den gesamten Incident Response lifecycle

SEC Consult
an atos company

Herausforderungen beim Incident Handling

SEC Consult
an atos company

Aus der Praxis

International (DACH) tätiges Unternehmen (Sitz: Deutschland)

Umsatz ca. EUR 500 Millionen

ca. 800 Mitarbeiter

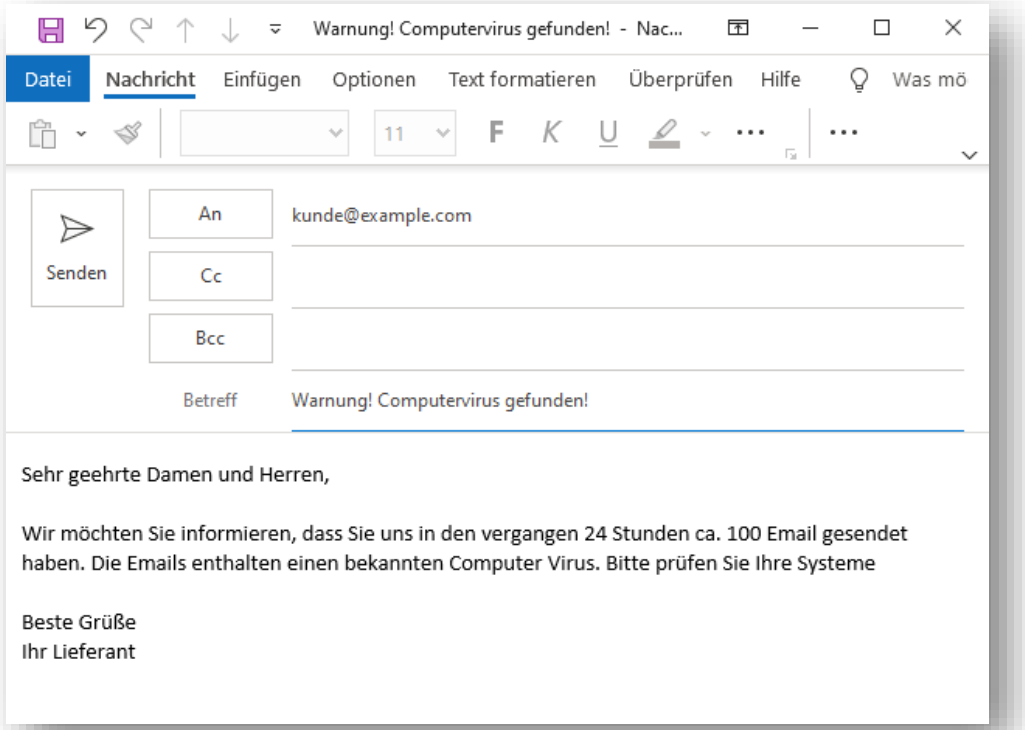
Jede Menge IT Systeme

Opfer eines Cyber Angriffs

SEC Consult
an atos company

Praxisbericht

Phishing Emails mit Malware werden
an **Kunden und Lieferanten** versendet



Alarmierungen von McAffee **Antivirus System**
34 Systeme verseucht -> Nicht mehr Einsatzbereit

Tag 0

Praxisbericht

Infektion außer Kontrolle
Über **200 Neuinfektionen** pro Tag

Produktionsstraße und
Logistik **außer Betrieb**

Erste Versuche die Infektion **selbstständig** unter Kontrolle zu bringen

- Systeme **löschen** und **wiederherstellen**
- Viele **Fragen**
- Viele **Überstunden**

Tag 0 — Tag 3

Praxisbericht

Externe Unterstützung angefordert
Viele Fragen vor dem Einsatzbeginn
- Was ist passiert?
- Was wurde bisher gemacht?
- Welche Mittel stehen zur Verfügung (Personal, Software, …)

Treffen mit Krisenteam - Abstimmung der Strategie
- **Eindämmung**
- Cyber-Triage - Schnelle Wiederherstellung der Produktion (**Priorisierung**)
- Identifikation der **Sicherheitslücken**

Tag 0 Tag 3 Tag 4

Praxisbericht

Herausforderung bei der Analyse

- ✓ (Fast) Alle User verfügten über **lokale Admin Rechte**
- ✓ Services werden mit **Domain-Administrator** Userkonten betrieben
- ✓ Mangelnde **Dokumentation** -> Was ist normal?

- ✓ Spurensuche war sehr schwierig, da (fast) **keine Logging** Funktionen eingesetzt werden

- ✓ Ausgangspunkt der Infektion (**Patient 0**) ist unbekannt

Praxisbericht

EMOTET
C:\Windows\<random>.exe as Service
Run Key for C:\Windows\SysWow64\<random>.exe

lateral movement

TROJAN-F (Keylogger, Exfiltration, Persistierung)
Run Key for
C:\Users\<User>\AppData\Romaing\somename.exe

CoreBot
Scheduled task that executes .dll via rundll32.exe

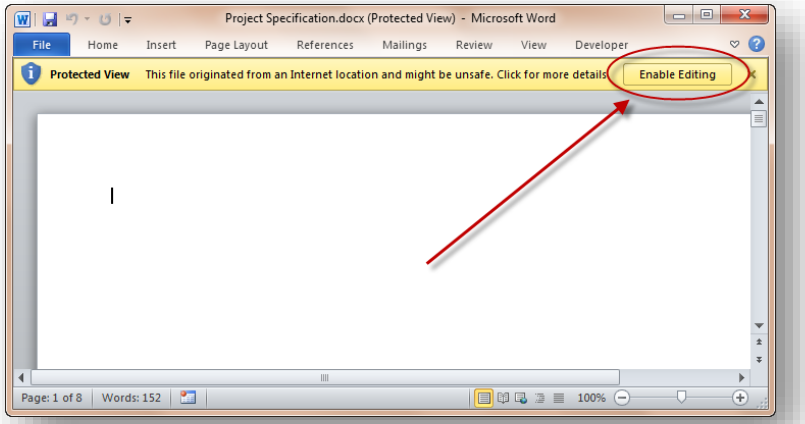
Payload:
- Sucht nach Banking Daten & Kunden-Daten

CryptoLock-D

Kryptolocker → Daten Verschlüsseln

Tag 0 Tag 3 Tag 4 Tag 8

Praxisbericht



Erkenntnisse

- ✓ Initiale Infektion über **Email mit einem WORD File (EMOTET)**
- ✓ Infektion bleibt **unbemerkt** weil:
  - ✓ Ungeschulter User klickt drauf
  - ✓ Vorfall wird von **User nicht gemeldet**

Erkenntnisse

- ✓ **Weiterverbreitung** via Lateral Movement
- ✓ Angreifer hat **Domain-Administrator** Rechte
- ✓ Versuch mittels Malware Banking Daten zu finden
- ✓ Exfiltration von Kunden-Daten
- ✓ Später: **Erpressungsversuch** mittels Kryptolocker

Tag 0 — Tag 3 — Tag 4 — Tag 8

SEC Consult
an atos company

Praxisbericht

Bereinigung der infizierten Systeme
- Aus Backup **wiederherstellen**
- Infektionswege **schließen**/abdichten
- Wechsel aller **Passwörter**

Stillstand in der **Produktion (ca. 4 Tage)**
Wiederholte Betriebsunterbrechungen für **Office Clients (ca. 2 Wochen)**
GDPR Meldepflicht / Verstoße (Datenverlust)
Reputationsschaden

Tag 0 | Tag 3 | Tag 4 | Tag 8 | Tag 20

Zusammenfassung

OBJECTIVE

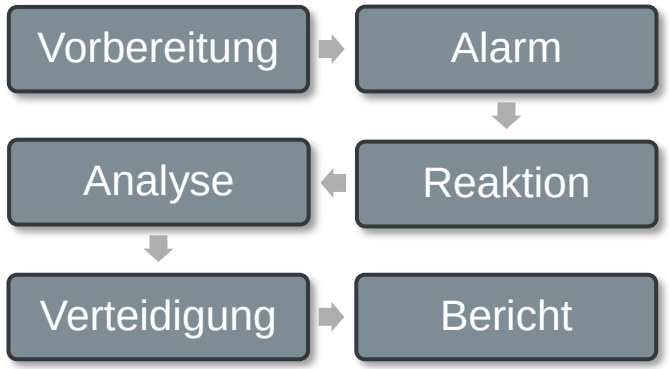
Schadensbegrenzung durch schnelle Reaktion auf einen Incident

Forensische Analyse des Incidents
Sicherung der gefundenen Beweise

Verhindern eines **erneuten Angriffs**

Rasches **Wiederaufnehmen** der regulären Arbeit

APPROACH



BENEFIT

Eindämmen von **finanziellen und Imageschäden**

Schutz von **sensiblen** Unternehmensdaten

Analyse der Ist-Situation des Unternehmens und Ableiten von individuellen **Maßnahmen**

SEC Consult +

Rapid Response Team mit Experten aus den Bereichen Forensik, Reverse Engineering, technischer und organisatorischer Informationssicherheit

24/7 Rufbereitschaft mit definierten Responsezeiten

Unterstützung durch ein **Off-Site Team**

50+ Incidents behandelt

SEC Consult
an atos company

Haben Sie noch Fragen?

Besuchen Sie unseren Messestand oder kontaktieren Sie uns direkt

CYBER INCIDENT? CALL +49 30 398 202 777

www.sec-consult.com

SEC Consult
an atos company

SEC Consult in Ihrer Region (DACH)

ÖSTERREICH - Wien

SEC Consult Unternehmensberatung GmbH
Leopold-Ungar-Platz 2, Stiege 3 / 3. OG
1190 Wien

Tel +43 1 890 30 43 0
Email office@sec-consult.com

ÖSTERREICH – Wiener Neustadt

SEC Consult Unternehmensberatung GmbH
Komarigasse 14/1
2700 Wiener Neustadt

Tel +43 2622 905 68
Email office-neustadt@sec-consult.com

ÖSTERREICH - Linz

SEC Consult Unternehmensberatung GmbH
Wienerstraße 131, Top 01.01.05
4020 Linz

Tel +43 1 890 30 43 0
Email office-linz@sec-consult.com

DEUTSCHLAND - Berlin

SEC Consult Deutschland Unternehmensberatung GmbH
Ullsteinstrasse 130, Turm B/8 Stock
12109 Berlin

Tel +49 30 398 20 2700
Email office-berlin@sec-consult.com

DEUTSCHLAND - München

SEC Consult Deutschland Unternehmensberatung GmbH
Palais Leopold, Leopoldstraße 12
80802 München

DEUTSCHLAND – Bochum

SEC Consult Deutschland Unternehmensberatung GmbH
Südring 25
44787 Bochum

DEUTSCHLAND – Nürnberg

SEC Consult Deutschland Unternehmensberatung GmbH
Königstorgraben 11
90402 Nürnberg

SCHWEIZ

SEC Consult (Schweiz) AG
Bändliweg 20/4. Etage
8048 Zürich

Tel +41 44 271 777 0
Email office-zurich@sec-consult.com

LUXEMBURG

SEC Consult Luxemburg S.ár.l.
246, rue de Beggen
L-1220 Luxemburg

Tel +352 621 493 221
Email office-luxembourg@sec-consult.com

SEC Consult
an atos company