



DIGITIZE YOUR BUSINESS

iT-Sicherheit im Mittelstand: Rückblick und Konsequenzen aus den letzten 12 Monaten iT-Sicherheitsberatung

Tobias Rademann, M.A.

2. Unternehmerabend der Stadt Gladbeck und des BVMW zum Thema Cybercrime und iT-Sicherheit
12. November 2019

Agenda

1. Kern-Trends der letzten 12 Monate
2. Konsequenzen



Kurzprofil: R.iT GmbH

- **Fokus:** iT-Unternehmensberatung für die Digitale Transformation
- **Kernthemen:** Digitalisierungsberatung
angewandte iT-Sicherheit
Geschäftsprozessautomatisierung
- **gegründet:** 2001, Spin-Off der Ruhr-Universität
- **Standorte** Zentrale: Bochum
Region Nord: Bad Schwartau
- **Zertifizierung:** BMWi-autorisiert für > iT-Sicherheit *und*
> digitale Geschäftsprozesse

EFQM: Recognized for **Digital Excellence*****

go-digital



Kern-Trends der letzten 12 Monate • Konsequenzen

Kern-Trends der letzten 12 Monate

Kern-Trends der letzten 12 Monate



Passgenauigkeit



Untätigkeit



Überforderung



Einschränkungen

Trend 1/4: Passgenauigkeit

Angriffe werden immer zielgerichteter:

- verseuchte eMails zu **echten Geschäftsvorfällen**
 - von Ihren Kontakten
 - an Ihre Kontakte
- Kenntnis über Ihre **Zugangsdaten**
- **Maximieren** der Schadenhöhe
- **maßgeschneiderte Höhe** der Erpressungsforderungen

→ Ansätze von APT (advanced persistent threat)



Exkurs: EMOTET

A blue L-shaped graphic element consisting of a vertical bar on the left and a horizontal bar on top, with a small teal triangle at the top right corner.

Erstinfektion

- durch SPAM-eMail mit Makro

Demo: Kompromittierung eines PCs mit SPAM



The screenshot shows an Outlook email interface. The top ribbon has tabs for 'Datei', 'Nachricht', and 'Was möchten Sie tun?'. The ribbon contains various icons for actions like 'Löschen', 'Antworten', 'Weiterleiten', 'Verschieben', 'Kategorisieren', and 'Suchen'. The email header shows the sender as 'Rolf Drescher' with the subject '[disarmed] Bewerbung als IT-System-Kaufmann'. The recipient is 'Jobs | R.i.T GmbH'. The email body contains two attachments: 'Nowak-Bewerbung.xls' (131 KB) and 'Nowak-Bewerbung.pdf' (133 KB). The text of the email is as follows:

Sehr geehrter Herr Bastian Nowak,

hiermit bewerbe ich mich bei Ihnen für die die Stelle als IT-System-Kaufmann. Meine vollständigen Bewerbungsunterlagen können Sie dem Anhang entnehmen.

Ich freue mich auf Ihre Rückmeldung und stehe Ihnen bei Rückfragen jederzeit gerne zur Verfügung.

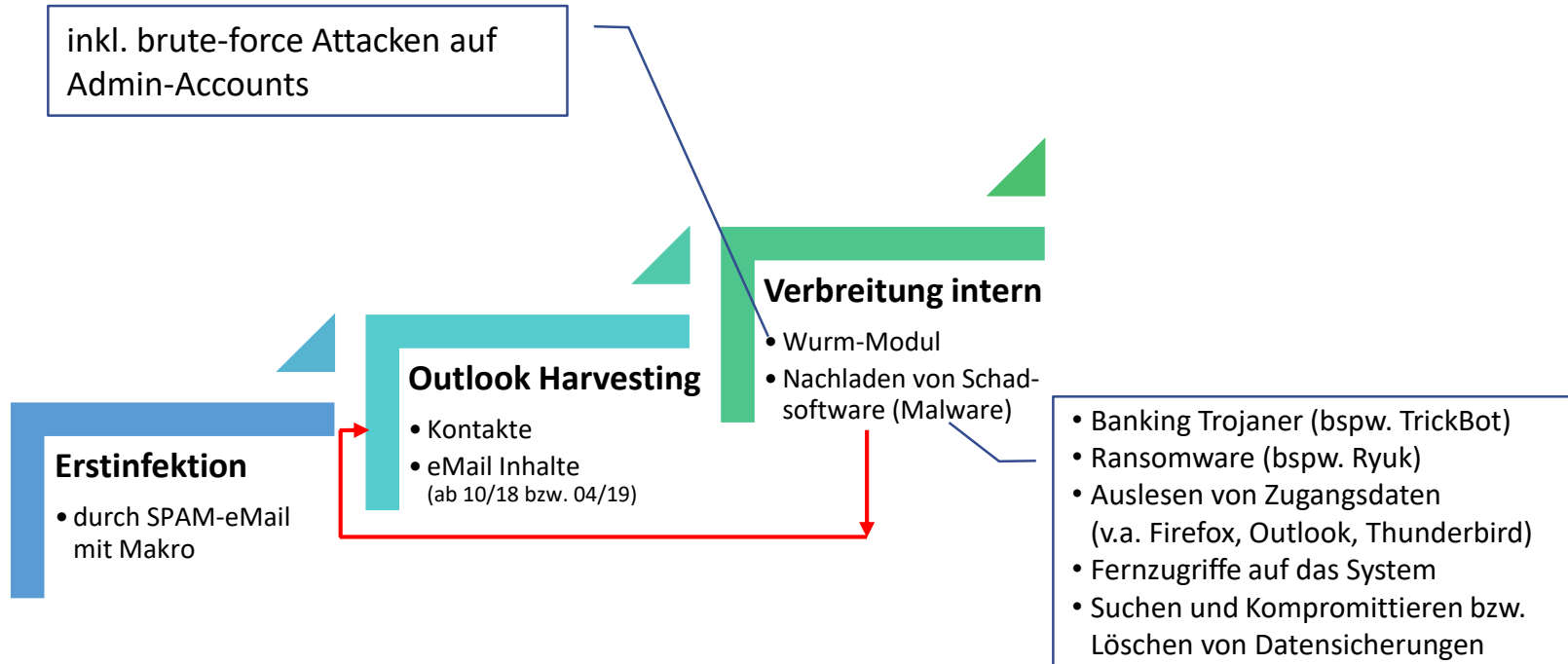
Mit freundlichen Grüßen

Rolf Drescher

Anmerkung:

An dieser Stelle wurde im Rahmen der Präsentation ein Video abgespielt, das die Infektion eines Arbeitsplatzes durch einen Erpressungstrojaner (Goldeneye) live zeigte.

Exkurs: EMOTET / I



Exkurs: EMOTET / II

bis hierhin: vom Unternehmen völlig unbemerkt!

BSI (2019): "die für die Empfänger (künftig) **kaum noch** als solche zu identifizieren sind"

Erstinfektion

- durch SPAM-eMail mit Makro

Outlook Harvesting

- Kontakte
- eMail Inhalte (ab 10/18 bzw. 04/19)

Verbreitung intern

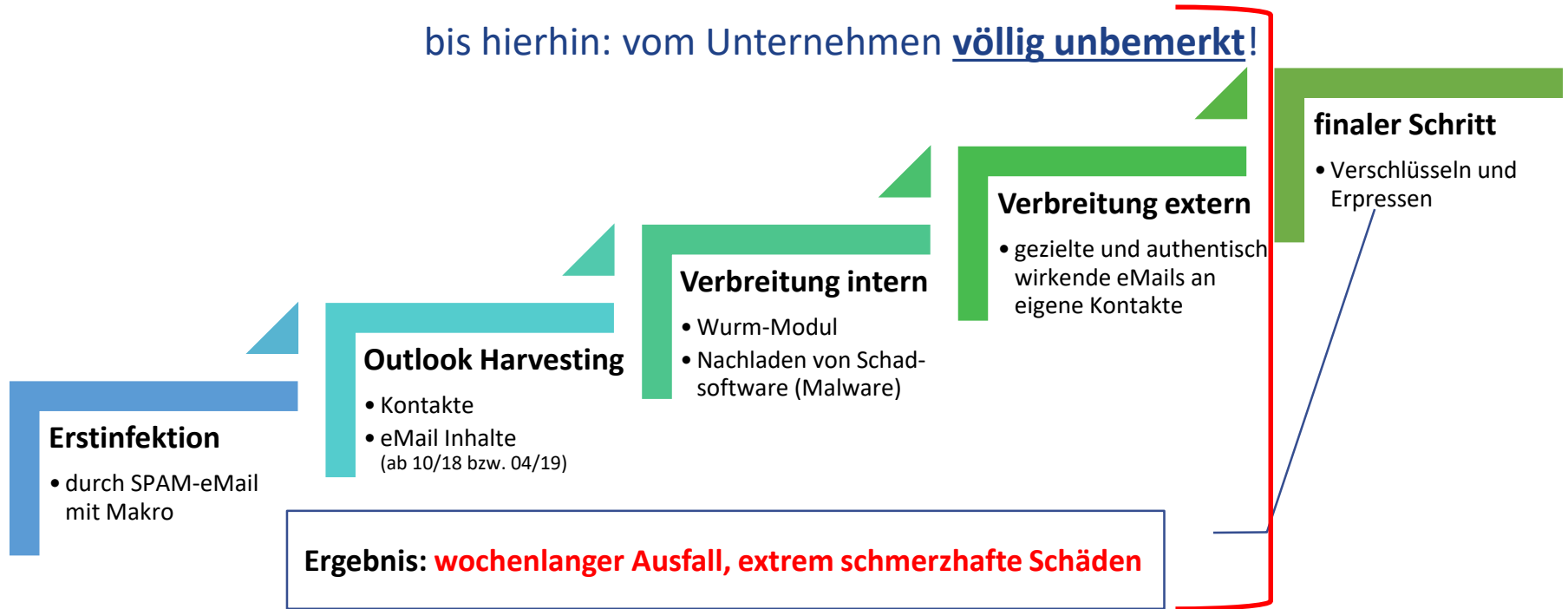
- Wurm-Modul
- Nachladen von Schadsoftware (Malware)

Verbreitung extern

- gezielte und authentisch wirkende eMails an eigene Kontakte

Exkurs: EMOTET

bis hierhin: vom Unternehmen völlig unbemerkt!



Trend 1/4: Passgenauigkeit / II

gleichzeitig:

- Konzerne investieren erheblich in iT-Sicherheit
- Mittelstand wird immer vernetzter
(Digitalisierung, Anforderungen Kunden, Lieferanten & Mitarbeiter)

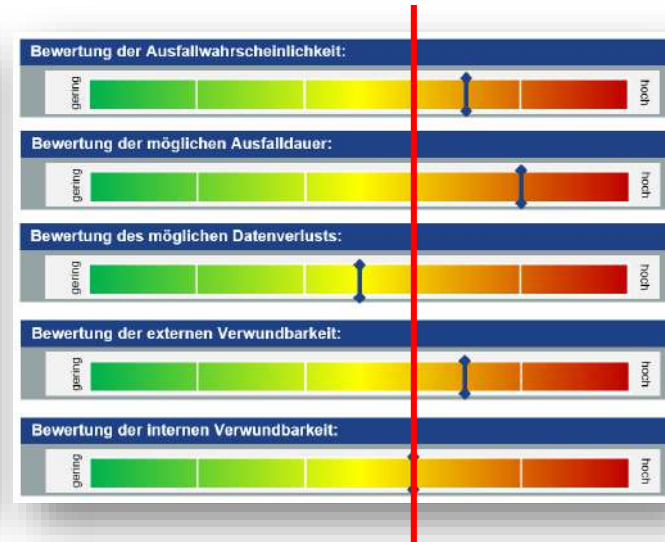
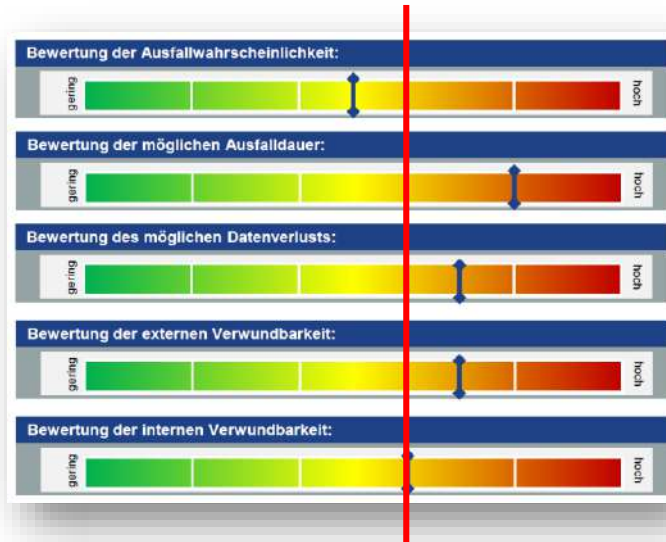
→ Mittelstand wird ein immer attraktiveres Opfer



Trend 2/4: Untätigkeit


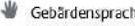
iT Sicherheit weitgehend reaktiv:

- Ergebnisse unserer iT Risk Assessments zeigen eklatante Lücken:



absoluter Basisschutz gegen CyberCrime



Service Kontakt  Leichte Sprache  Gebärdensprache

Teilnehmer werden Inform

Maßnahmen zum Schutz vor Emotet und gefährlich

Folgende Maßnahmen **MÜSSEN** aus Sicht des **BSI** innerhalb de

- Regelmäßige Information und **Sensibilisierung von Nutzern** für die Gefahren d... auch bei vermeintlich bekannten Absendern (siehe auch gefälschte Absenderad... heruntergeladene Dateien im Zweifel nur nach Rücksprache mit dem Absender... sollten Auffälligkeiten umgehend an den **IT-Betrieb** und den **IT-Sicherheitsbez**
- Zeitnahe Installation von den Herstellern bereitgestellte **Sicherheitsupdates** für Web-Browser, Browser-Plugins, E-Mail-Clients, Office-Anwendungen, **PDF-D** zentrale Softwareverteilung.
- Einsatz zentral administrierter **AV-Software**. Regelmäßige Prüfung, ob Updates werden.
- Regelmäßige Durchführung von mehrstufigen **Datensicherungen (Backups)**, ins... auch die Planung des Wiederanlaufs und ein Test der Rückspielung von Daten.
- Regelmäßiges manuelles **Monitoring** von Logdaten, idealerweise ergänzt um automatisiertes Monitoring mit Alarmierung bei schwerwiegenden Anomalien.



WIKIPEDIA
Die freie Enzyklopädie

Hauptseite
Themenportale
Zufälliger Artikel

 Nicht angemeldet [Diskussionsseite](#) [Beiträge](#) [Benutzerkonto erstellen](#) [Anmelden](#)

Artikel [Diskussion](#) [Lesen](#) [Bearbeiten](#) [Quelltext bearbeiten](#) [Versionsgeschichte](#)

Emotet

Emotet ist ein Computer-Schadprogramm in Form eines sogenannten „Banking-Trojaners“, das auf modernere Versionen des Betriebssystems Windows von Microsoft abzielt, und ist i. d. R. dem Bereich der **Ransomware** zugeordnet. Dabei ist es auf das Abfangen von **Online-Banking-Zugangsdaten** spezialisiert, kann darüber hinaus jedoch noch eine Vielzahl weiterer Module mit anderen Schadfunktionen nachladen und zur Ausführung bringen.^[1] Opfer der Schadsoftware sind vor allem Behörden und Unternehmen.

Gegenmaßnahmen [\[Bearbeiten | Quelltext bearbeiten \]](#)

Vor der Infektion [\[Bearbeiten | Quelltext bearbeiten \]](#)

Grundvoraussetzung für alle Schutzmaßnahmen ist das **Einspielen aktueller Sicherheits-Updates**^[1] und das Vorhandensein von aktueller **Backups**, die physisch vom Netzwerk getrennt sind.^[2] Als direkte Gegenmaßnahme kann die Ausführung von **Makros** per **Gruppenrichtlinie** im **Active Directory** komplett deaktiviert werden –, sollte das nicht möglich sein, so kann zumindest nur die Ausführung von **signierten Makros** per **Gruppenrichtlinie** zugelassen werden.^[9] Word Anhänge können zur Prüfung auch z. B. in **LibreOffice** geöffnet werden, denn dort funktionieren die Makros nicht.^[6] Da Passwörter aus **Firefox** und **Outlook**, bzw. **Thunderbird** ausgelesen werden, wird die Verwendung eines **Passwortmanagers** empfohlen. Arbeiten mit reduzierten Benutzerrechten (keine Adminrechte) v. a. beim Surfen im Internet und beim Öffnen von E-Mail Anhängen ist sinnvoll, um zu verhindern, dass eine Infektion der Systemdateien erfolgt. Für administrative Konten werden starke Passwörter empfohlen, da Emotet diese mit **Brute-Force-Methoden** zu ermitteln versucht.^[9]

häufigste Schwachstellen in 2019

- **Lücken in der Datensicherung**
 - online verfügbar (keine physikalische Trennung)
 - unzureichende Historie
 - unverschlüsselt



häufigste Schwachstellen in 2019

- Lücken in der Datensicherung
- **Lücken bei Sicherheitsupdates (Patches)**
 - Arbeitsplätze fehlen
 - nicht Microsoft-Software nicht berücksichtigt
 - unregelmäßig ("nur, wenn mal Zeit ist")
 - ungesteuerte / unüberwachte (d.h. automatische) Updates im Backend



häufigste Schwachstellen in 2019

- Lücken in der Datensicherung
- Lücken bei Sicherheitsupdates (Patches)
- keine (regelmäßige) Sensibilisierung der Anwender
- **viel zu laxer Rechteverwaltung**
 - Nutzung von Standardkennworten, v.a. für Peripherie (ThinClients, Switches, Drucker, etc,)
 - leichter Zugriff auf sensible Unternehmensdaten (ERP Systeme, BWAs, Personaldaten)
 - Speichern von Kennworten im Browser und in Mailprogrammen wie Outlook, Thunderbird



häufigste Schwachstellen in 2019

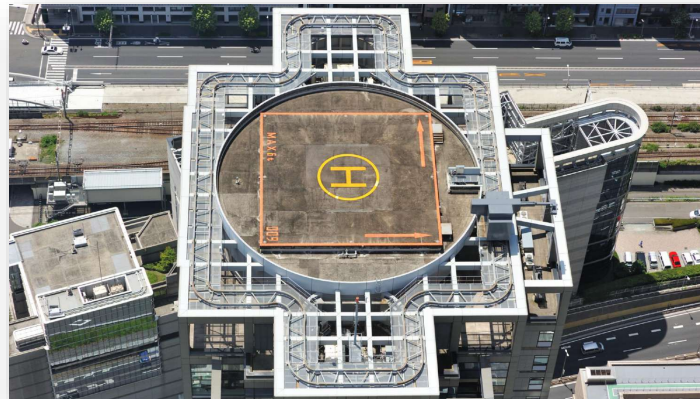
- Lücken in der Datensicherung
- Lücken bei Sicherheitsupdates (Patches)
- keine (regelmäßige) Sensibilisierung der Anwender
- viel zu laxer Rechteverwaltung
- keine ganzheitlichen Blicke auf die zentralen Systeme (= Wartungen)
- keine Disaster Recovery Tests, (Notfall-)Dokumentation oder Notfallkonzepte
- keine Systemüberwachung ('Monitoring')



Trend 2/4: (Un)tätigkeit

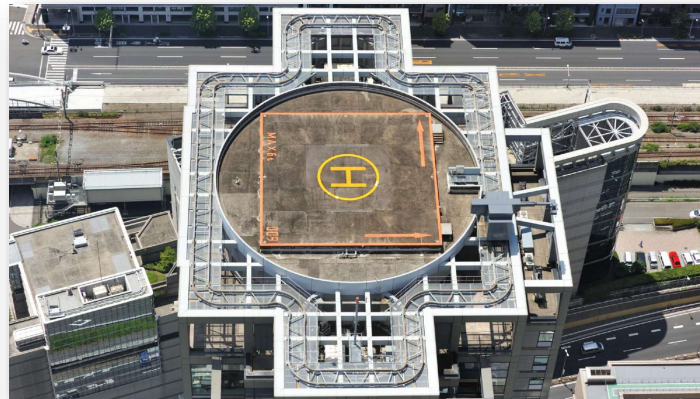
- **Beispiel: Industrie 4.0-Werk**

- Mitarbeiter bauen aktiv eine Zielscheibe / einen Landeplatz: eigenen AccessPoint an Switch im Industrie-Netzwerk geklemmt, um mit dem Handy WLAN zu haben (in der Halle ist kein Mobilfunknetz...)



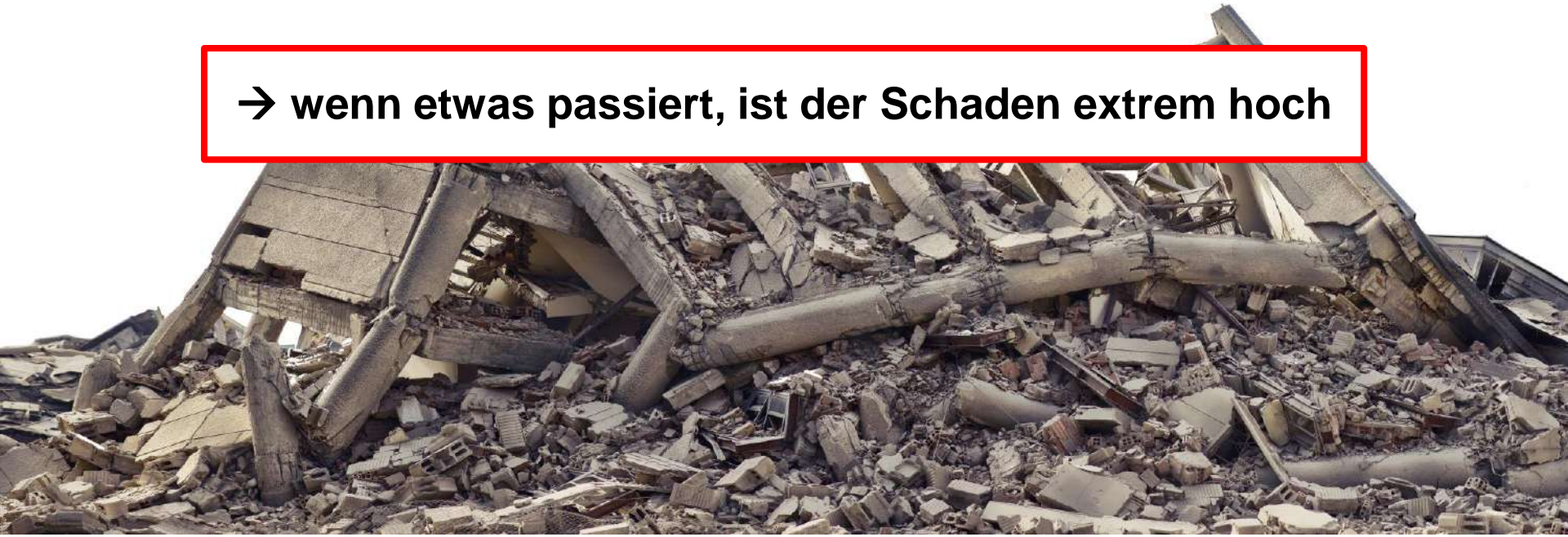
Trend 2/4: (Un)tätigkeit

- Beispiel: Industrie 4.0-Werk
- **Beispiel: Einzelhandel**
 - Lieferung für Neukunden auf Rechnung
 - keine Überprüfung der Identität



Trend 2/4: Untätigkeit – Konsequenz

→ wenn etwas passiert, ist der Schaden extrem hoch



Trend 3/4: Überforderung

iT Sicherheit überfordert viele:

- **Anbieter**
 - ✓ Kreditkartenbetrug: Bank – Aufnahme nicht möglich, weil kein Schaden entstanden
 - ✓ Identitätsdiebstahl: Polizei – Aufnahme der Anzeige (angeblich) nicht möglich, weil kein Schaden entstanden
- **Betroffene** (Firmen, Individuen): Wissen nicht, was sie tun sollen/können
- **iT-ler**
 - ✓ viele Kollegen überfordert
 - ✓ falsch verstandene Rollen/Anforderungen
interne iT-ler: Koordinator (!), **nicht** Allround-Experte



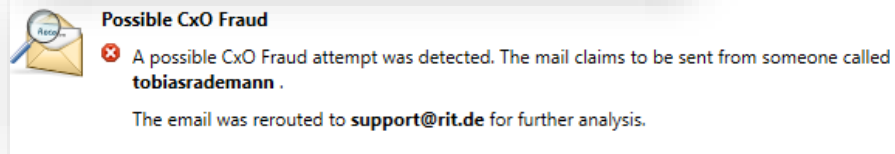
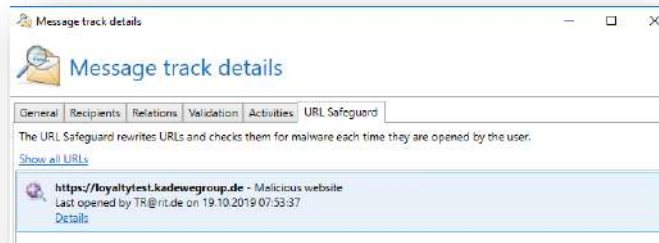
Trend 4/4: Einschränkungen

das Korsett wird enger:

- immer mehr Falschmeldungen ('false positives')
- korrekte Erkennung ausgefeilter Angriffe wird immer schwerer
- die Einschränkungen bei der Arbeit nehmen zu

Beispiele aus 2019:

- CEO-Fraud
- malicious links



Trend 4/4: Einschränkungen

das Korsett wird enger:

- immer mehr Falschmeldungen ('false positives')
- korrekte Erkennung ausgefeilter Angriffe wird immer schwerer
- die Einschränkungen bei der Arbeit nehmen zu

→ Lernen / Erfahrung sammeln ist zentral

- technisch: Konfiguration von iT-Sicherheitssoftware
- organisatorisch: Sensibilisierung für Auswirkungen von iT-Schutz / Umgang mit 'false positives'



Kern-Trends der letzten 12 Monate • **Konsequenzen**

Konsequenzen

Résumé der letzten 12 Monate

Angriffe werden **individueller** – damit **steigt das Risiko erheblich**
gleichzeitig
noch immer **viele Lücken** (oft dieselben, oft grundlegende!)

→ Handeln Sie – **jetzt!**

Konsequenzen: Handeln Sie – *jetzt!*

1. sorgen Sie für eine Grundlage

- regelmäßige Sicherheitsupdates
- physisch getrennte, regelmäßige Backups
- regelmäßige Sensibilisierung von Anwendern

2. machen Sie iT-Sicherheit zur Gewohnheit

- proaktiv
- zielgerichtet
- regelmäßig

3. arbeiten Sie mit Experten

→ mit kleinen aber kontinuierlichen Schritten viel erreichen

Vielen Dank für Ihre Zeit und Ihre Aufmerksamkeit!

Bei Rückfragen wenden Sie sich gerne an:



DIGITIZE YOUR BUSINESS

Tobias Rademann, M.A.

R.iT GmbH • www.RiT.de

Zentrale: Amtmann-Ibing-Str. 10, 44805 Bochum

Tel.: (0234) 43 88 00-0, Fax: -29

NL Nord: Tremskamp 5, 23611 Bad Schwartau

Tel.: (0451) 203 68-500, Fax: -499

eMail: Tobias.Rademann@RiT.de