DIGITIZE YOUR BUSINESS

Zielscheibe Mittelstand:
Rückblick auf die letzten 12 Monate iT-Sicherheitsberatung

Tobias Rademann, M.A.

DIGITAL FUTUREcongress Essen
5. 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

Ludwig Erhard Preis
Recognised for Digital Excellence

Kern-Trends der letzten 12 Monate

Kern-Trends der letzten 12 Monate

Passgenauigkeit

Untätigkeit

Überforderung

Einschränkungen

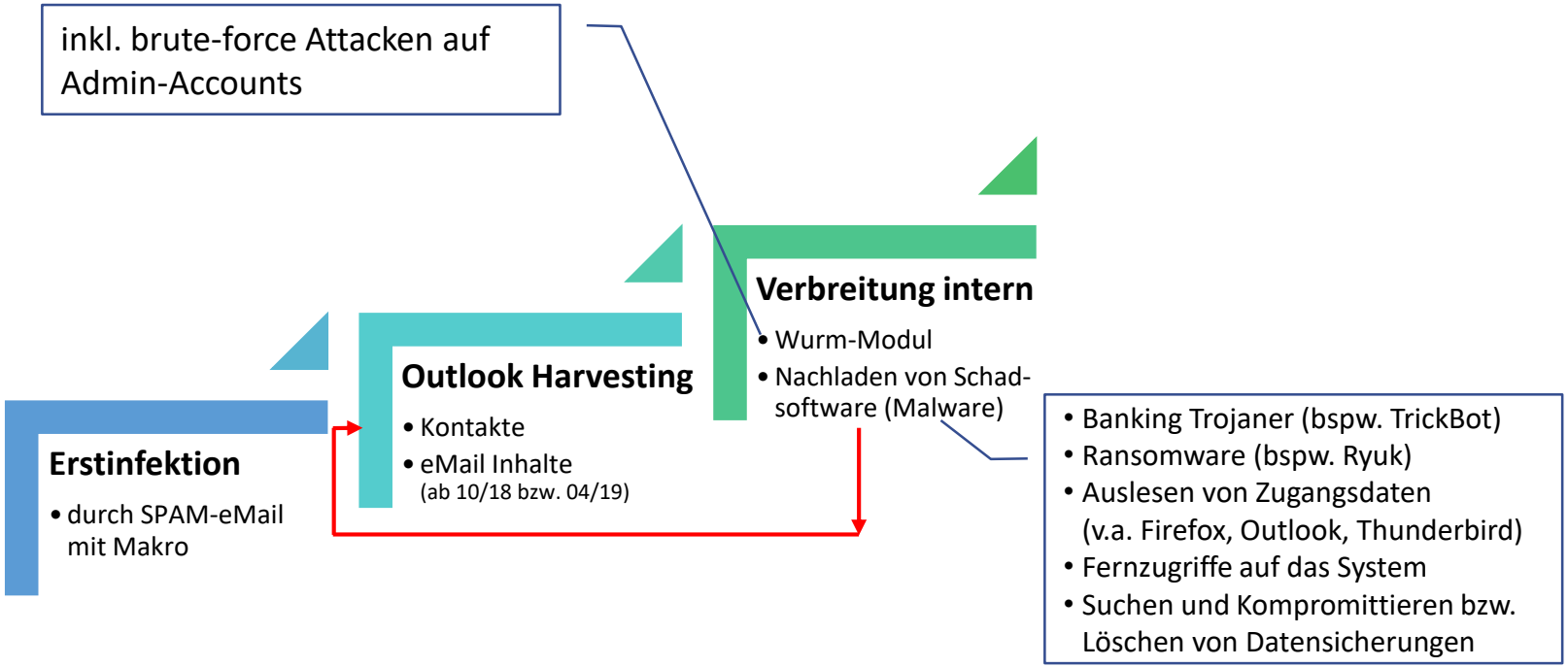
Trend 1/4: Passgenauigkeit

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)

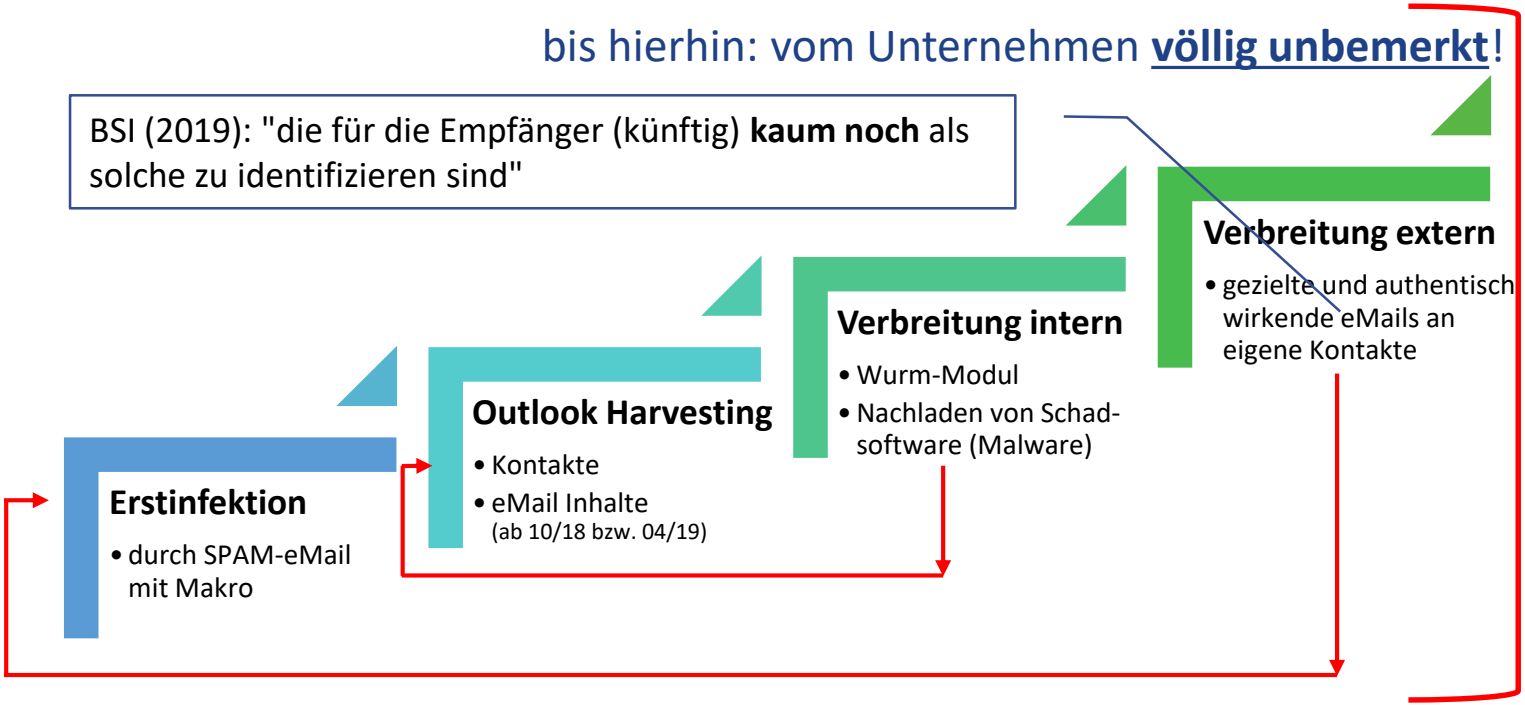
Exkurs: EMOTET / I



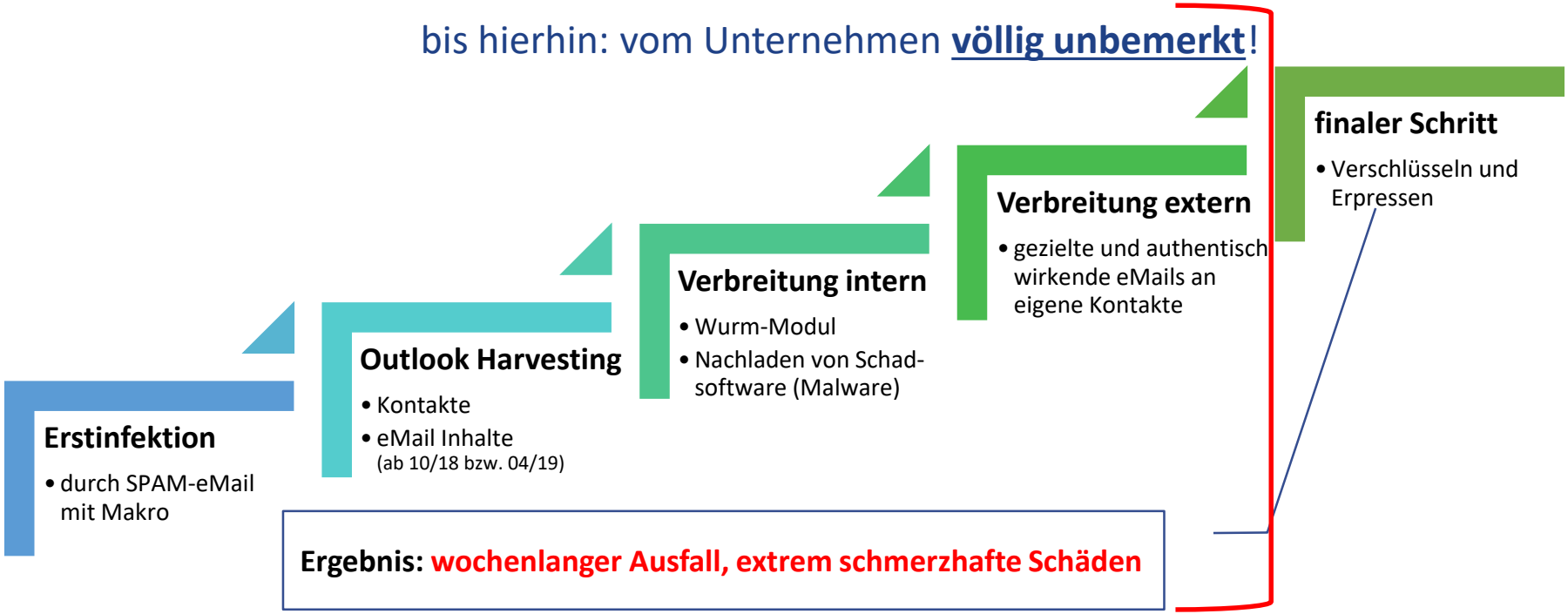
Exkurs: EMOTET / II

bis hierhin: vom Unternehmen **völlig unbemerkt**!

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



Exkurs: EMOTET



Trend 1/4: Passgenauigkeit / II

gleichzeitig:

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

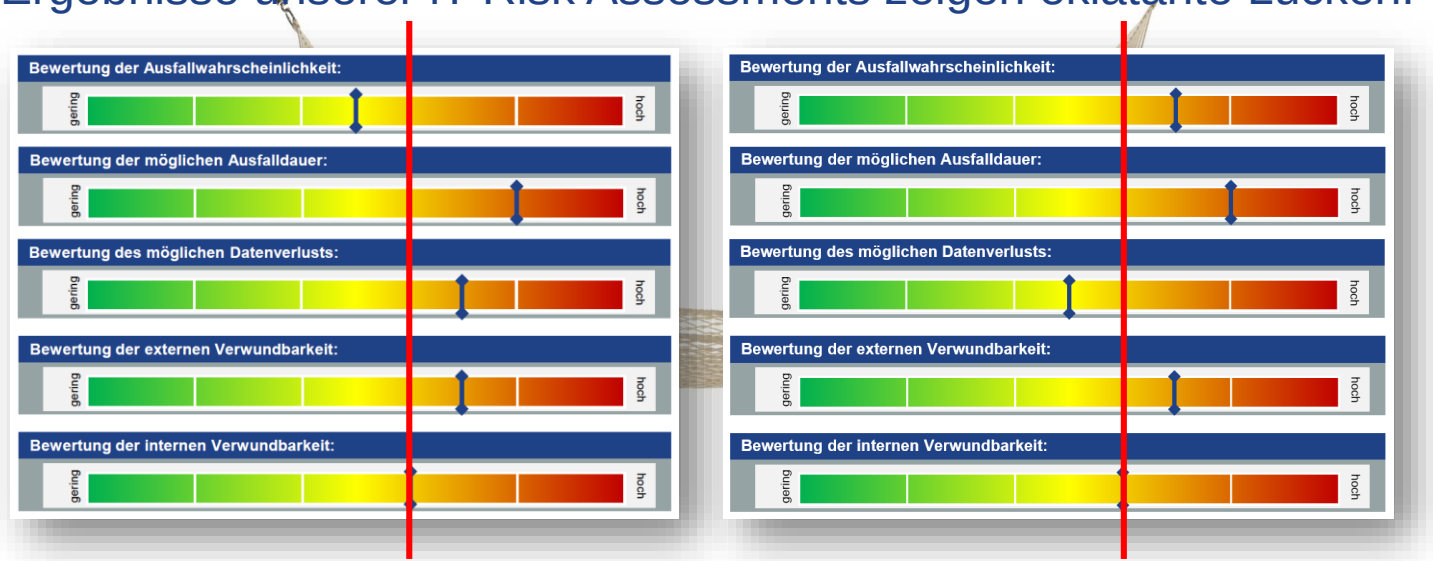
→ Mittelstand wird ein immer attraktiveres Opfer


MAX6t
009

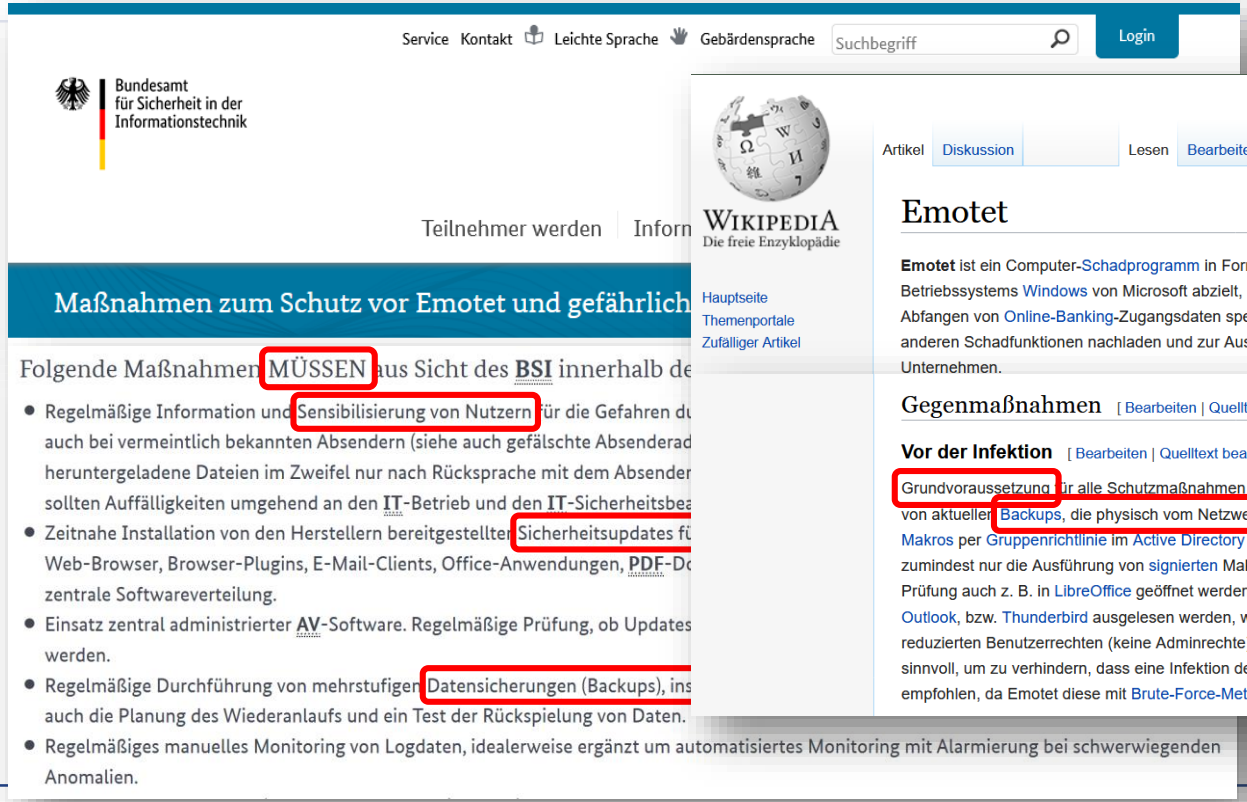
Trend 2/4: Untätigkeit

iT Sicherheit weitgehend reaktiv:

- Ergebnisse unserer iT Risk Assessments zeigen eklatante Lücken:



absoluter **Basisschutz** gegen CyberCrime



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

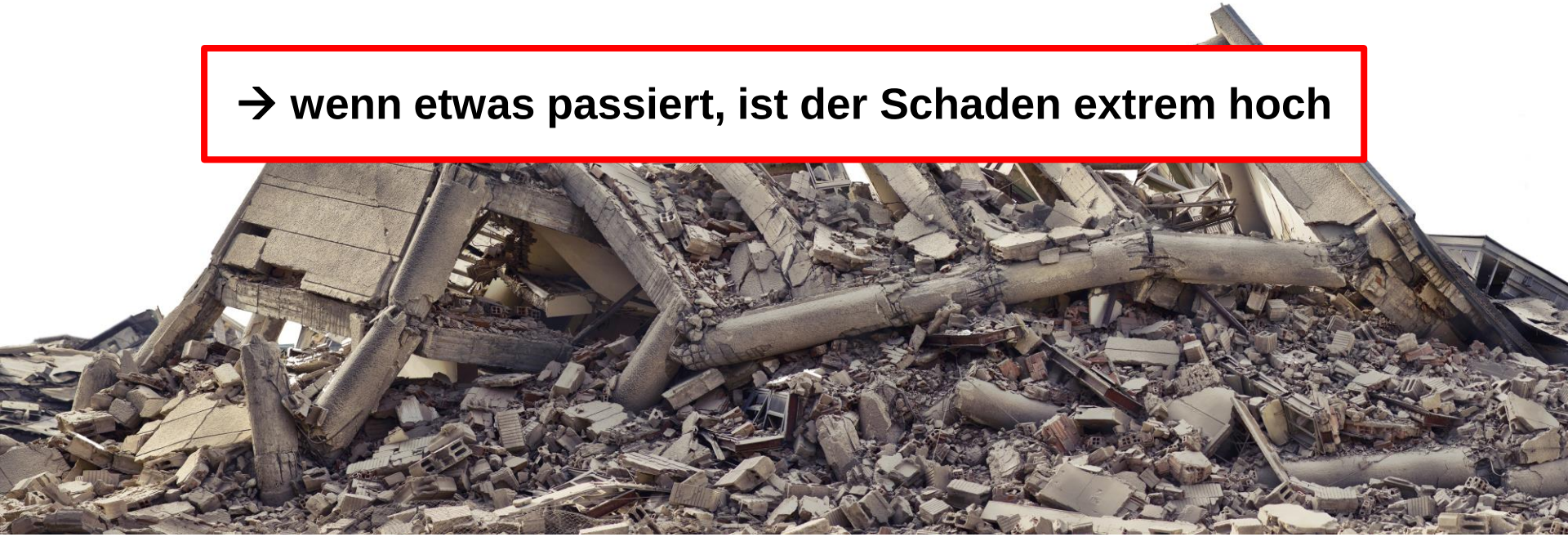
- Lücken in der Datensicherung
- Lücken bei Sicherheitsupdates (Patches)
- keine (regelmäßige) Sensibilisierung der Anwender
- **viel zu laxe Rechteverwaltung**
  - Nutzung von Standardkennworten, v.a. für Peripherie (ThinClients, Switches, Drucker, etc,)
  - leichter Zugriff auf sensible Unternehmensdaten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

häufigste Schwachstellen in 2019

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

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

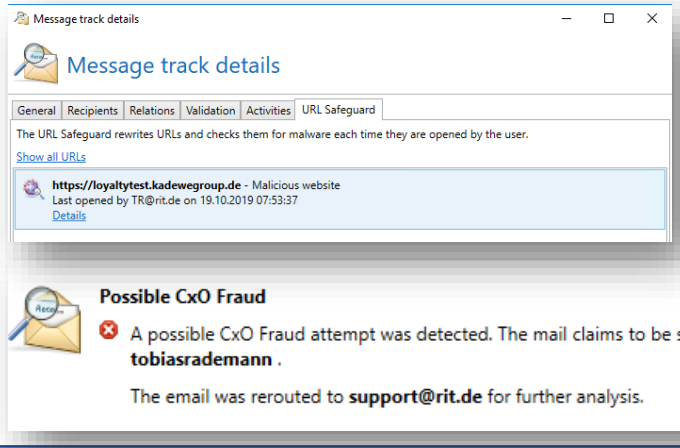
Trend 4/4: Einschränkungen

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'

Konsequenzen

Résumée 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

offene Fragen / Diskussion

Sprechen Sie uns gerne hier vor Ort an:
Stand E13

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

Ludwig Erhard Preis
Recognised for Digital Excellence