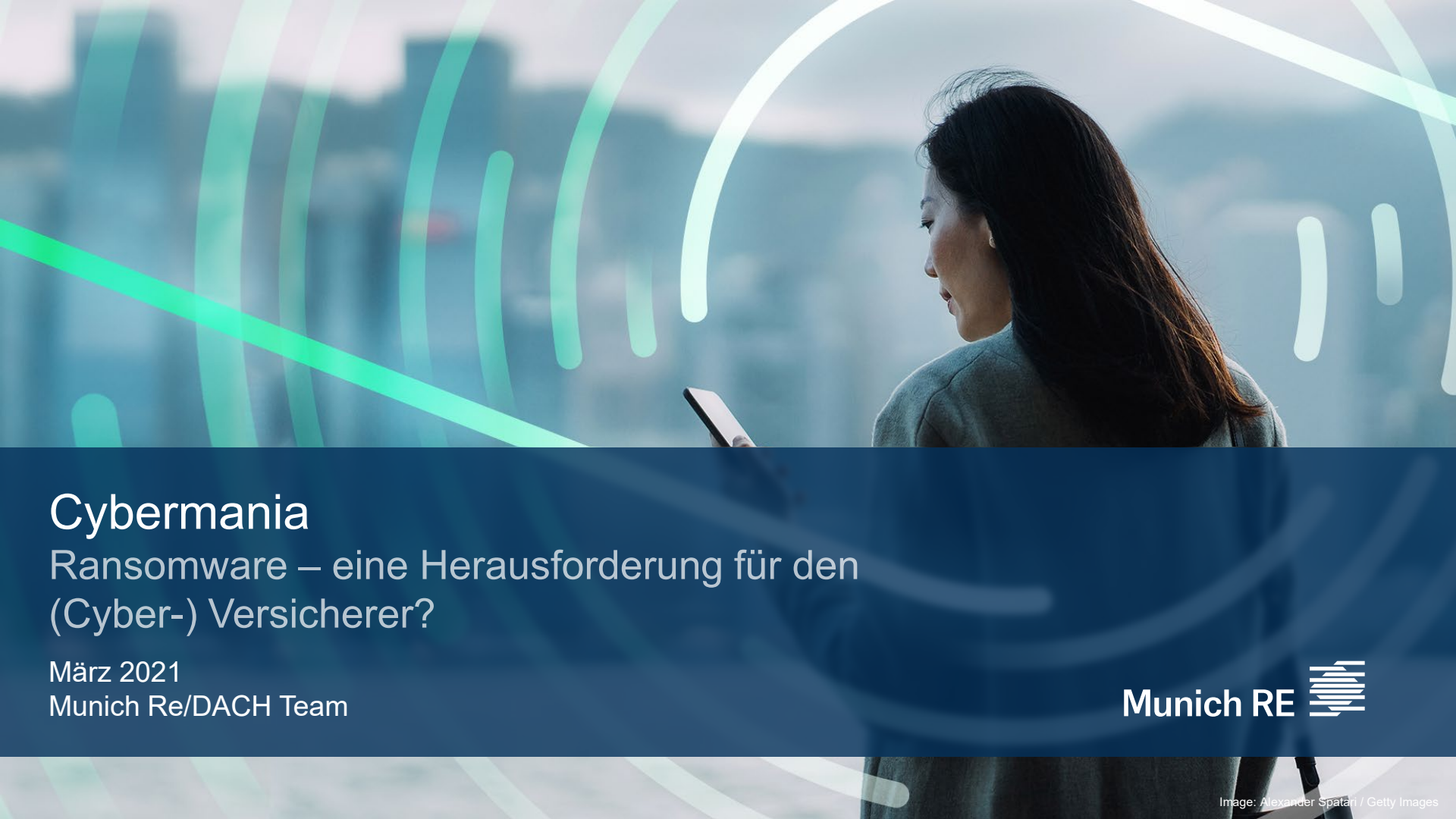


Cybermania

Ransomware – eine Herausforderung für den (Cyber-) Versicherer?

März 2021

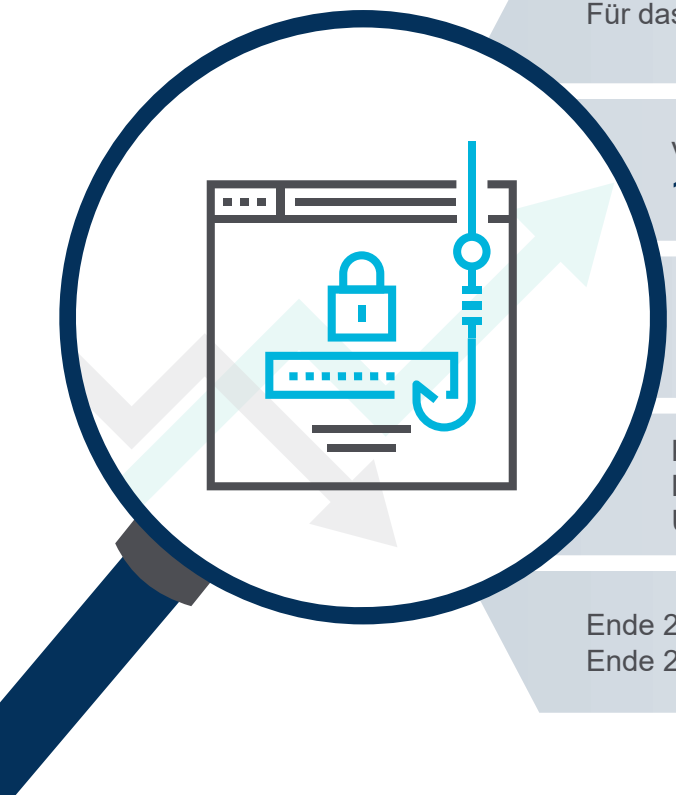
Munich Re/DACH Team

Munich RE

Image: Alexander Spatari / Getty Images

Ransomware Statistiken und Entwicklungen 2020

Munich RE



Für das 2. Quartal schätzt Coveware die durchschnittlichen Lösegeldforderungen auf **$178,000**

Von allen Ransomware Attacken im 2. Quartal 2020 trafen **55%** Firmen mit weniger als **100 Mitarbeitern** und **75%** trafen Unternehmen mit weniger als **$50m** Gewinn

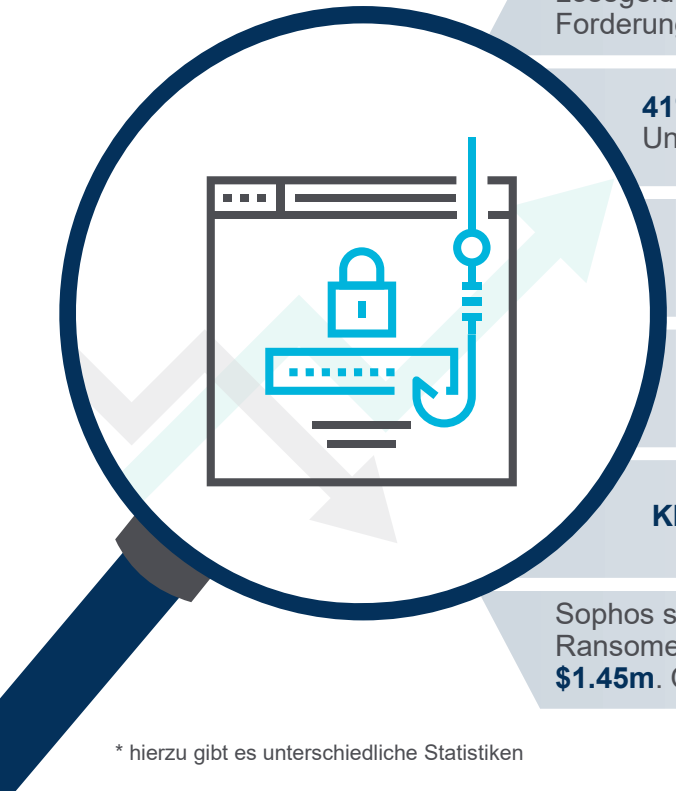
Sophos schätzt, daß **73%** aller Ransomware Attacken erfolgreich verlaufen

Kosten für Betriebsunterbrechung können genauso hoch ausfallen wie Kosten für Lösegeldforderungen. In 2020 lagen die durchschnittlichen Kosten für die Unterbrechung bei insgesmt **$283,000 -** und damit **100%** höher als noch in 2019

Ende 2019 haben Cyberkriminelle mit Ransomware **$11.5bn** „verdient“.
Ende 2020 wird ein Anstieg auf **$20bn** erwartet

Ransomware Statistiken und Entwicklungen 2020

Munich RE



Lösegeldforderungen **steigen exponentiell**. In einigen Fällen stellte die IBM Security X-Force Forderungen von mehr als **$40m** fest

41% aller von IBM Security X-Force analysierten Ransomware Attacken in 2020 trafen Unternehmen mit **“Operational Technology“ (OT)** Netzwerken

Industrie, Dienstleistung, Behörden und das Gesundheitswesen sind die **beliebtesten Opfer** in 2020. Auch viele Akademische und Forschungseinrichtungen standen im Visier!

“**Leak and Shame”** Taktik: Durch den Diebstahl von Unternehmens-Daten erweitern sich Ransomware Attacken immer öfter auch zu Datenschutzverletzungen

KMUs leiden überproportional stark unter Ransomware Attacken

Sophos schätzt, dass sich durch Zahlungen von Lösegeldforderungen die Kosten durch Ransomeware-Attacken verdoppeln. Wurde Lösegeld bezahlt, lagen die Kosten im Schnitt bei e bei **$1.45m**. Ohne Lösegeld lagen die Durchschnittskosten bei **$730,000***

* hierzu gibt es unterschiedliche Statistiken

Ransomware: Die weiteren Aussichten …

Schäden durch Ransomware Attacken werden auch in 2021 weiter **rapide steigen**. Insbesondere der Verlust von Daten und gestohlenen Passwörter stehen im Vordergrund.

Durch die Kombination dieser **"decrypt and delete"** Forderungen werden sich Schadenkosten verdoppeln.

Cyberkriminelle drohen mit der Veröffentlichung von Daten (**e-store of stolen databases),** wenn Forderungen nicht beglichen werden.

Expert-level Ransomware operators/Big Game Hunters und Entry-level Attackers setzten sich auf der Suche nach potentiellen Angriffsmöglichkeiten zunehmend ab.

Sicherheitsexperten vermuten, das sich **der weltweite Gesamtschaden durch Ransomware-Kosten in 2021 auf $20bn belaufen kann.** Das wäre 57 mal höher als noch in 2015.

Politisch könnte das Thema in 2021 an Fahrt aufnehmen, insbesondere weil mittlerweile auch der Behörden sowie kritische Infrastrukturen ins Visier der Angreifer gerückt sind.

Munich RE

Bedeutung für Versicherer? Wichtig!

- Lösegeldforderungen orientieren sich an Versicherungssummen! Wie geht man als Versicherunhsindustrie damit um?
- 2021! Wir und unsere Kunden müssen uns vorbereiten! Das heißt:
  - ✓ Netzwerksegmentierung
  - ✓ Aktueller, getesteter und funktionierender Incidence Response Plan
  - ✓ sichere Backup Prozesse müssen implementiert und getestet sein
  - ✓ …
- Risikoappetit, Kumulmodelle, Preise und Risikoprüfung müssen angepasst werden

Diskutieren Sie mit uns!

Munich RE

Wie sind **Ihre** Prognosen hinsichtlich Ransomware-Schäden

Wie können **wir gemeinsam** Versicherungsnehmer dabei unterstützen, sich vor diesen Angriffen zu schützen

Wie können **Dienstleister** dazu beitragen, diesen Teufelskreis zu durchbrechen

Diskutieren Sie mit uns!

Was müssen wir an unserem **Underwriting** prozess anpassen

Was müssen wir jetzt umsetzen, um Cyberversicherung **nachhaltig profitabel** zu machen

Was kann effektives **Schadenmanagement** dazu beitragen

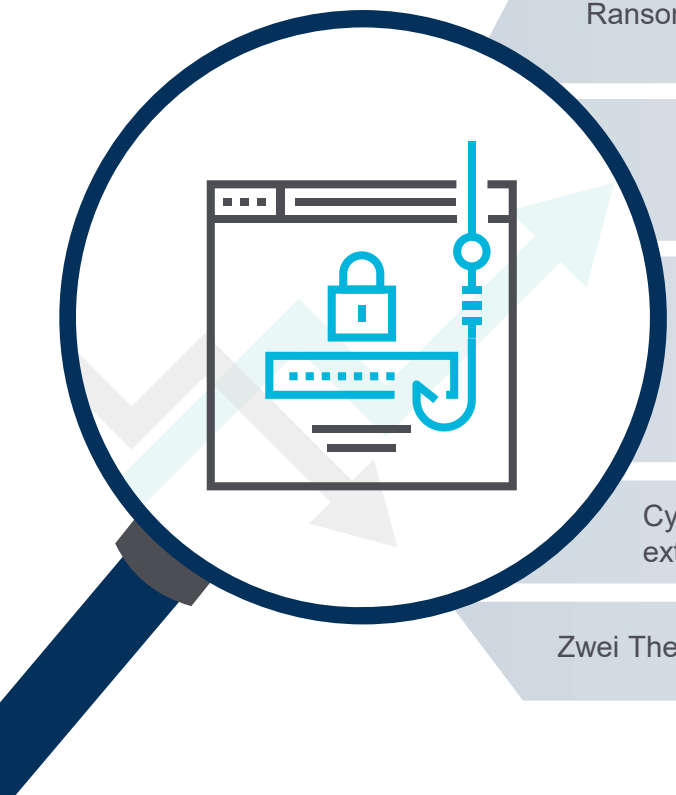
Ransomware trifft auch KMU

Munich RE

Company	Industry	Country	Employees	Revenue $	Attack Date	Attack Type
Alphacam	IT - Software	Germany	111	21 Mio	January 2021	Ransomware
AppliChem GmbH	Manufacturing	Germany	83	17 Mio	October 2020	Ransomware
Berzelius Stolberg GmbH	Manufacturing	Germany	23	50 Mio	December 2020	Ransomware
Autohaus Muhra GmbH	Automotive	Germany	-	-	March 2021	Ransomware
CISEG GmbH	Manufacturing	Germany	500-1000	-	March 2021	Ransomware
Delme-Werksttten für Behinderte gGmbH	Healthcare	Germany	6	1 Mio	March 2021	Ransomware
Autohaus Niggemeier	Automotive	Germany	-	-	August 20	Ransomware
Handelshof Stendal GmbH	Retail	Germany	114	30 Mio	October 2020	Ransomware
IRLE Deuz GmbH	Manufacturing	Germany	23	4 Mio	January 2021	Ransomware
MAT GmbH	Automotive	Germany	24	4 Mio	December 2020	Ransomware

Unsere Erfahrungen mit Ransomware-Schäden

Munich RE



Ransomware-Attacken werden aufwendiger. Schäden werden teurer.

Notwenige technische Schritte bei der Handhabung von Ransomware-Attacken:
Identifikation, Eindämmung, Beseitigung, Wiederherstellung, (Empfehlungen)

Betroffene Deckungsbestandteile:

- Forensik / Schadenfeststellungskosten
- Wiederherstellung von Daten und Programmen
- Betriebsunterbrechung / Ertragsausfall / Mehrkosten
- Benachrichtigungskosten

Cyberversicherung / Schadenbearbeitung mit technischem Sachverstand (intern und extern)

Zwei Themen im Fokus: Incident Response und Obliegenheiten

Obliegenheiten in Cyber-Policen

Munich RE

GDV Allgemeine Versicherungsbedingen Cyber

- **Unterscheidung einzelner Nutzer und Befugnisebenen** (individuelle Zugänge für alle Nutzer mit ausreichend komplexen Passwörtern). Administrative Zugänge sind ausschließlich Administratoren und ausschließlich zur Erledigung administrativer Tätigkeiten vorbehalten
- **Schutz gegen unberechtigten Zugriff** (Firewall, 2-Faktor-Authentifizierung bei Servern, Verschlüsselung von Datenträgern mobiler Geräte, Diebstahlsicherung oder ähnlich wirksame Maßnahmen)
- **Schutz gegen Schadsoftware**, der automatisch auf dem aktuellen Stand gehalten wird (z. B. Virenscanner, Code Signing, Application Firewall oder ähnlich wirksame Maßnahmen)
- **Patch-Management**, das eine unverzügliche Installation von relevanten Sicherheitspatches sicherstellt
- mindestens wöchentlicher **Sicherungsprozess**, wobei die Sicherungsdatenträger physisch getrennt aufbewahrt werden. Im Versicherungsfall darf auf Originale und Duplikate nicht gleichzeitig zugegriffen werden können.

Obliegenheiten in Cyber-Policen

Munich RE

1. Versicherer nutzen Obliegenheiten in Cyber-Policen zur
   - Disziplinierung von Versicherungsnehmern
   - Vermeidung des Eintritts von Versicherungsfällen
   - Risikominimierung
   - Ersparnis eines adäquaten Risk Assessments
2. Bewertung der Risikominimierung wird nicht vor Eintritt des Versicherungsfalls gelöst, sondern in die Schadenabteilung verlagert
3. Schadenabteilung ist abhängig von
   - vollständiger forensischer Analyse mit Fokus auf Obliegenheitsverletzungen
   - eindeutigem Policenwording
   - rechtlichen Rahmenbedingungen beim Ablehnen oder Kürzen von Versicherungsleistungen
4. Kaum Präzedenzfälle zur Bemessung des Verschuldensgrades bei der Kürzung der Versicherungsleistung (grobe Fahrlässigkeit?)
5. Bestehen erhöhte Sorgfaltspflichten für bestimmte Versicherungsnehmer (z.B. Unternehmen, die persönliche Daten verarbeiten)?

Diskutieren Sie mit uns!

Munich RE

Wie sind **Ihre** generellen Erfahrungen hinsichtlich der Inanspruchnahme von **durch Versicherer vorgeschlagenen** Dienstleistern

Wie sind **Ihre** Erfahrungen in der Schadenbearbeitung hinsichtlich des Einsatzes von **nicht durch Versicherer vorgeschlagenen Dienstleistern**

Wie sind **Ihre** Erfahrungen hinsichtlich der Regulierung von Incident Response Kosten

Diskutieren Sie mit uns!

Sind **Obliegenheitsverletzungen** ein Thema in Ihrer Schadenbearbeitung

Was sind **Ihre** Erfahrungen bei der Geltendmachung von Obliegenheitsverletzungen

Was sind **Ihrer Meinung nach** die aktuellen Themen bei der Bearbeitung von Cyberschäden?

Danke für Ihre wertvollen Beiträge!

März 2021
Munich Re/DACH Team

Munich RE

Image: Alexander Spatari / Getty Images