Marsh Medical Consulting

Cyber Risiken im Gesundheitswesen: Gefahren - Maßnahmen

Tag der Patientensicherheit – Medizinische Hochschule Hannover MHH

09. September 2021

Ingo Gurcke, Geschäftsführer – Marsh Medical Consulting
Leona Stege, Senior Fachbetreuerin – CYRIS / Healthcare Champion

Cyber Risiken

Schadenbeispiele aus der Vergangenheit

Frankfurter Allgemeine
ZEITUNG FAZ.NET

HACKERANGRIFF AUF KRANKENAKTEN

Tausende von Menschen öffentlich entblößt

In Finnland haben Hacker psychotherapeutische Krankenakten in großem Ausmaß geraubt. Neben der Angst vor Erpressung wächst die Sorge, ob ein ausländischer Geheimdienst dahinter steht. Für die digitale Euphorie ist diese Katastrophe eine Ernüchterung.

Quelle: faz.net, 28.10.2020

heise online

FBI warnt vor Cyberattacken auf Krankenhäuser in den USA

Laut IT-Sicherheitsexperten wollen Cyberkriminelle rund 400 Gesundheitseinrichtungen mit Erpressungstrojanern in die Bredouille bringen.

Quelle: heise.de, 29.10.2020

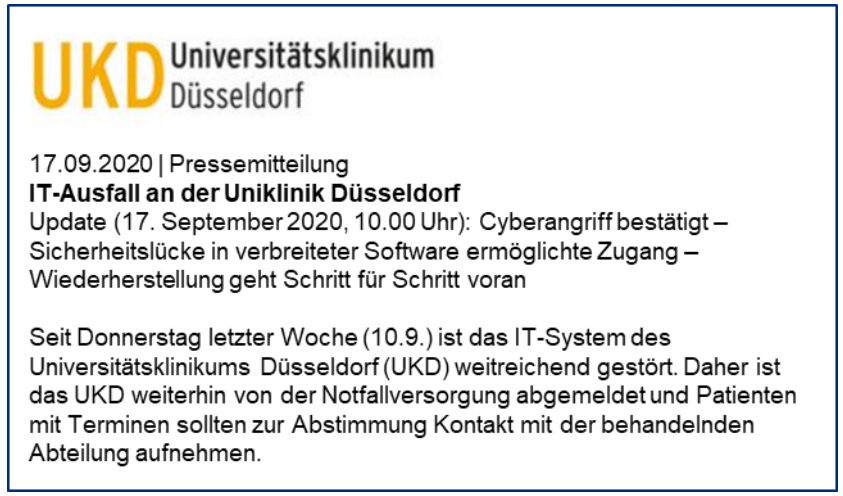
ÄrzteZeitung

Schlamperei bei Datensicherung

300.000 Patientendaten geklaut

Befunde, Patientendaten, Arztbriefe: Im Kreiskrankenhaus Rastatt sind Datenträger mit Patientenakten gestohlen worden. Für die Klinik ist der Fall schon jetzt teuer geworden.

Veröffentlicht: 12.10.2012, 15:37 Uhr



UKD Universitätsklinikum Düsseldorf

17.09.2020 | Pressemitteilung
IT-Ausfall an der Uniklinik Düsseldorf
Update (17. September 2020, 10.00 Uhr): Cyberangriff bestätigt – Sicherheitslücke in verbreiteter Software ermöglichte Zugang – Wiederherstellung geht Schritt für Schritt voran

Seit Donnerstag letzter Woche (10.9.) ist das IT-System des Universitätsklinikums Düsseldorf (UKD) weitreichend gestört. Daher ist das UKD weiterhin von der Notfallversorgung abgemeldet und Patienten mit Terminen sollten zur Abstimmung Kontakt mit der behandelnden Abteilung aufnehmen.

Agenda

- Cyber Risiken
- Risikomanagement Ansatz
- Versicherungsmarkt
- Zusammenfassung / Key takeaways

Cyber Risiken

Die Zahl und Komplexität der Angriffe nehmen zu

Aus unserer Datenbank

Die Schadenmeldungen wegen Erpressungssoftware **verdoppelten** sich 2019.

Allein in 2019 und 2020 verzeichnete Marsh Deutschland **versicherte** Schäden durch Ransomware in Höhe von voraussichtlich **EUR 33 Mio**. Bis 2019 betrug die Schadenhöhe aller bis dahin gemeldeten Schäden insgesamt nur EUR 325.000.

Aus anderen Quellen

Die weltweiten Gesamtkosten verursacht durch Ransomware werden 2021 voraussichtlich EUR 17 Mrd. übersteigen
(Quelle: cybersecurityventures.com)

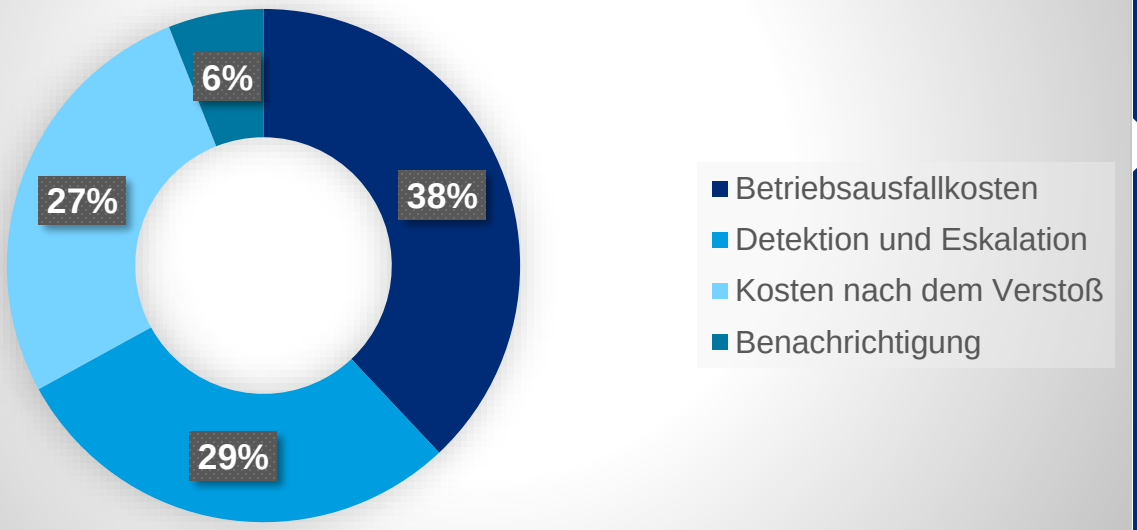
Durchschnittliche Ausfallzeit: 21 Tage
(Quelle: coveware.com)

Das Gesundheitswesen hatte in 2021 die höchsten Kosten für Datenschutzverstöße: durchschnittlich ca. EUR 7,8 Mio. (30% Steigerung im Vergleich zu 2020)
(Quelle: CODBR 2021, Ponemon Institute and IBM Security)

Cyber Risiken

Spotlight: Datenschutzverstöße

Durchschnittliche Gesamtkosten eines Datenschutzverstoßes unterteilt in Kostenkategorien



(Quelle: CODBR 2021, Ponemon Institute and IBM Security)

Angriffsvektoren (Häufigkeit)

1. Kompromittierte Zugangsdaten
2. Phishing
3. Fehlkonfiguration der Cloud

Angriffsvektoren (Kostenintensiv)

1. Kompromittierung von Geschäfts-E-Mails
2. Phishing
3. Böswilliger Insider

Cyber Risiken

Komplexität des Risikos

- Datenmanagement (Art, Anzahl und Ort der gespeicherten Daten; Klassifizierung)
- Sich kontinuierlich ändernde Bedrohungen und Risiken (z.B. Ransomware, Denial of Service Attacken)
- Täter und Auslöser (Staaten, Kriminelle, Terroristen, Mitarbeiter, Bedienungsfehler, Hackerangriff etc.)
- Dienstleister (Teilen von sensiblen Informationen, Outsourcing, Vertragsmanagement)
- Regulatorisches Umfeld (z.B. EU-Datenschutz Grundverordnung, ITSiG2.0, BSI)
- Technologischer Fortschritt (Cloud- und Mobile-Computing, Block Chain, Big Data, Social Media)
- Kritische Infrastrukturen/ Black Swans
- Zukunft der IT-Sicherheitstechnologien

Risikomanagement Ansatz

Risikomanagement Ansatz

Rahmenwerk zum Management von Cyber-Sicherheit

Vor dem Schaden

- **Transparenz** über Risiken **schaffen**
- **Maßnahmen** zur **Risikoverringerung** ableiten und umsetzen
- **Restrisiken transferieren**

Während des Schadens

- **Angriffe entdecken**
- **Angriffe abwehren**
- Rechtliche und wirtschaftliche **Interessen sichern**

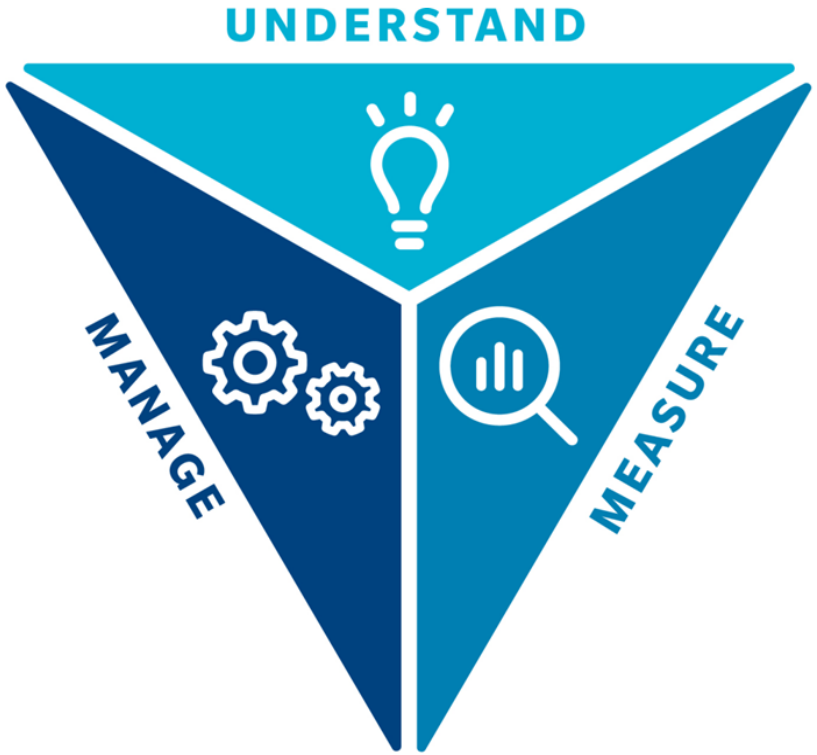
Nach dem Schaden

- **Entschädigung** sicherstellen
- **Ursachen** feststellen
- **Verbesserungen** ableiten

Quelle: NIST Security Framework, MARSH

Risikomanagement Ansatz

Voraussetzungen für ein effektives Risikomanagement



Understand: Übertragen Sie Cyber Risiken auf Ihren Betrieb, um Ihr individuelles Risiko zu identifizieren und zu verstehen.

Measure: Quantifizieren Sie die potentiellen Auswirkungen der Risiken.

Manage: Ergreifen Sie die notwendigen Maßnahmen zur Risikosteuerung. „secure | insure | recover“

Risikomanagement Ansatz

Understand | Grundwerte der Informationssicherheit

Vertraulichkeit

„Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.“

Integrität

„Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten“ angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.“

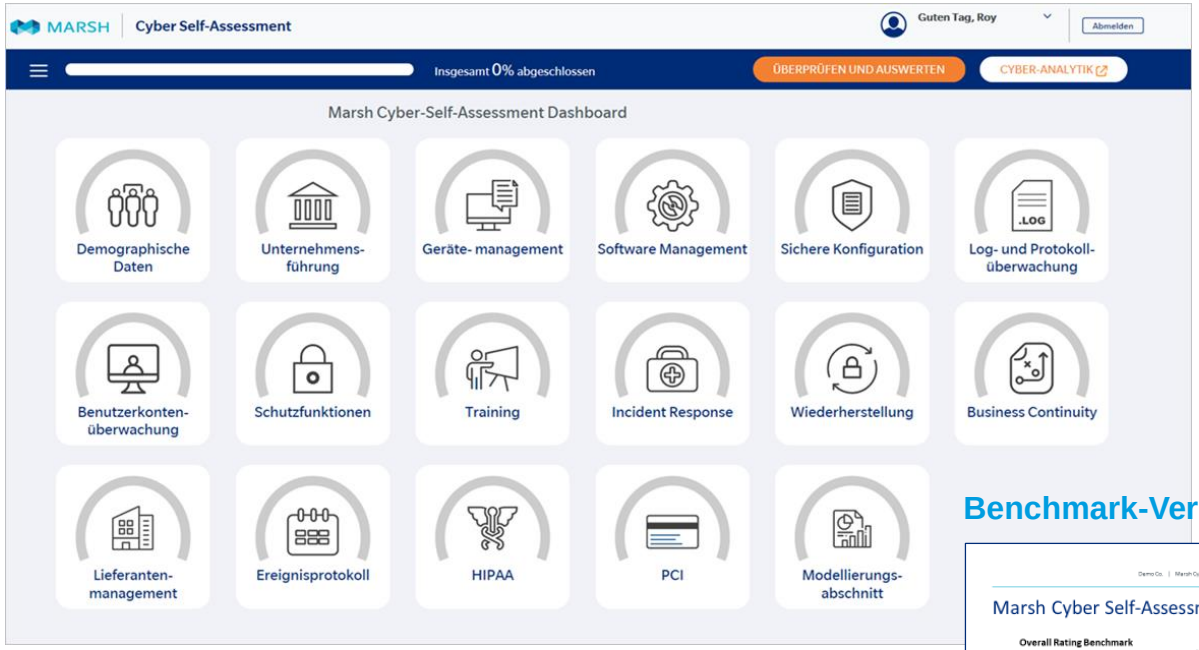
Verfügbarkeit

„Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.“

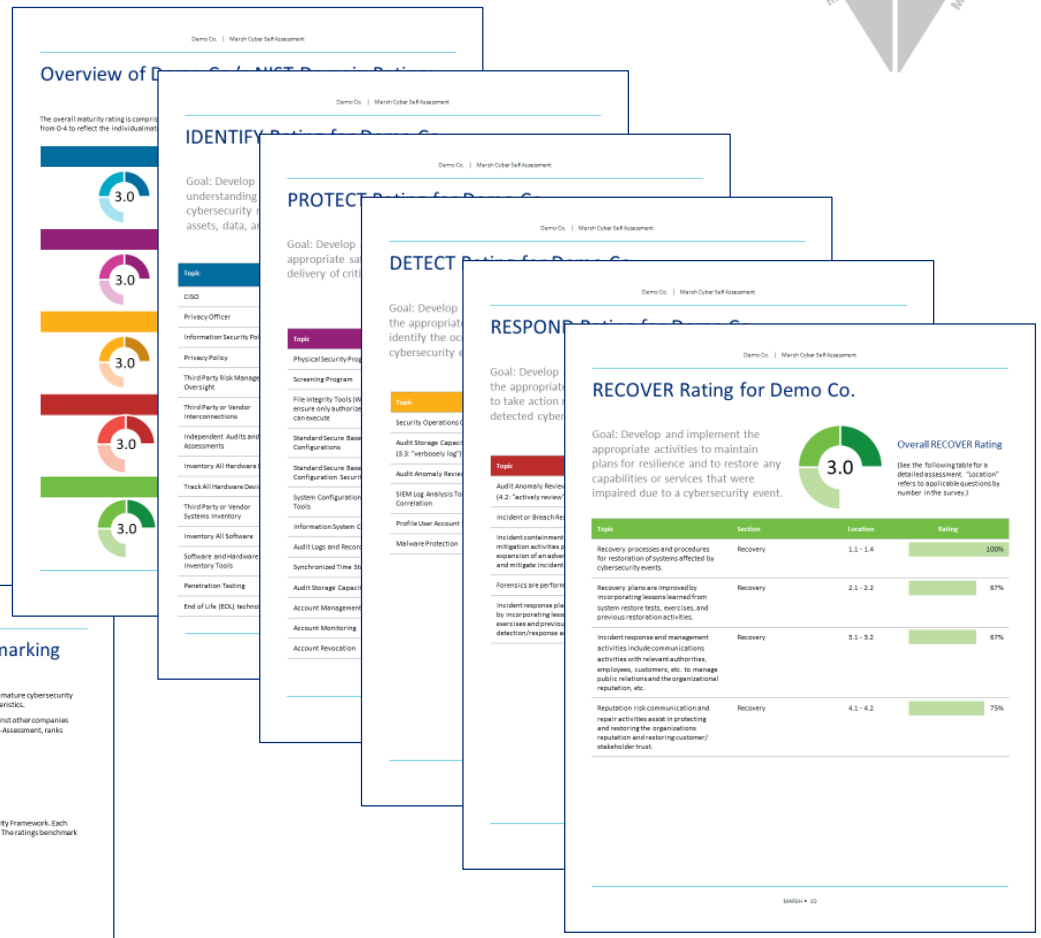
Quelle: Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium

Risikomanagement Ansatz

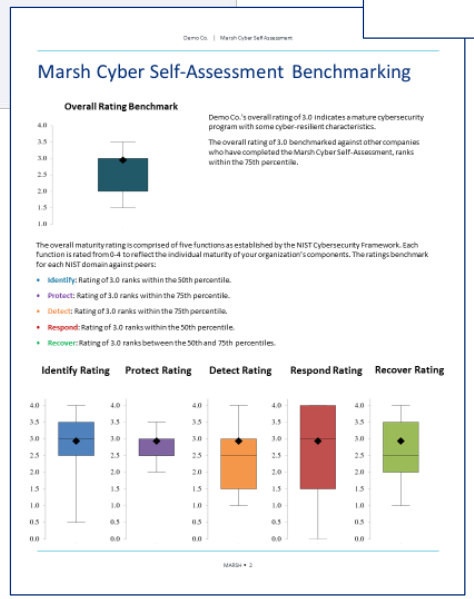
Understand | Reifegradbestimmung



Detaillierte Ergebnisse



Benchmark-Vergleich



Risikomanagement Ansatz

Measure | Quantifizierungsansatz

Vorsatztat

oder

Fahrlässigkeit,
Bedien-/Systemfehler

Informationssicherheitsverletzung

Vertraulichkeit Integrität Verfügbarkeit

Betriebsunterbrechungsschaden

zzgl. Mehraufwand
wie z.B. das Anmieten von Servern

Kosten & Aufwendungen

z.B. IT-Forensik, Rechts-, PR-Beratung,
Wiederherstellungskosten,
Erpressungsgelder u.v.m)

Haftpflichtansprüche

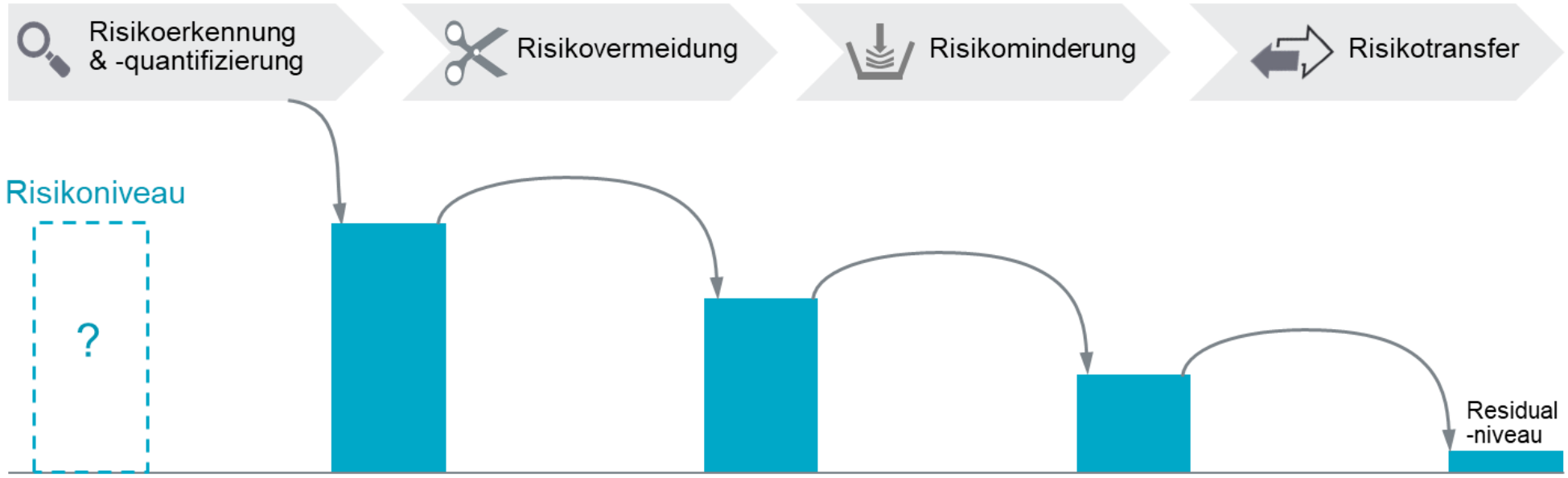
aus der Verletzung der
Informationssicherheit eines Dritten

Assistance Leistungen

Zurverfügungstellung von
Krisendienstleistungen wie IT-Forensik,
Rechts-und PR-Beratung über VR

Risikomanagement Ansatz

Manage | Steuerung des erkannten Risikos



Beitrag einer Cyber-Gefährdungsanalyse

- Identifikation und Quantifizierung spezifischer Cyber-Risiken
- Aufzeigen verwundbarer Geschäftsprozesse
- Aufzeigen möglicher Mitigierungsmaßnahmen
- Versicherbarkeitsanalyse identifizierter Risiken

Versicherungsmarkt

Versicherungsmarkt

Herausforderungen in der Informationssicherheit

- Krankenhäuser sind in der Regel frei zugänglich, potentielle Angreifer können sich verhältnismäßig leicht Zugang zu den Systemen verschaffen.

- Die zunehmende Digitalisierung führt zu einer Vielzahl von vernetzten, medizinischen Geräten, die angreifbar sind.

- Die Systeme sind selten voneinander getrennt, damit z.B. Untersuchungsergebnisse ohne Zeitverlust angezeigt, geteilt oder weitergeleitet werden können.

- Zeitdruck – eingehende Mails können nicht immer ausreichend auf Authentizität geprüft werden.

Versicherungsmarkt

Marktentwicklung Cyber

Versicherer

- 35 Cyber-Versicherer in Deutschland
- Hiervon zeichnen ca. 10 Versicherer grds. Cyberrisiken im Gesundheitswesen
- Hohe Mindestanforderungen an die Informationssicherheit

Schäden

- Schadenmeldungen nehmen weiter zu
- Komplexität nimmt zu
- Ransomware größte Bedrohung

Prämien

Jahr	RoL in CE
2019	1,05%
2020	1,32%
2021	1,45%

- Prämien werden voraus-sichtlich auch 2021 steigen

Underwriting

- Versicherer zeichnen noch restriktiver
- Versicherungsschutz wird an Auflagen geknüpft
- Versicherer verlangen Detaillierte Informationen
- Die Selbstbehalte werden stark nach oben angepasst

Underwriting: Spotlight Ransomware

Versicherbarkeit hängt zunehmend von der Informationssicherheit ab

Kritische Cybersecurity Controls:

- Multi-Faktor-Authentifizierung (MFA) für Remote- und Admin-Zugriff
- Endpoint Detection & Response
- Prozess oder Protokollierung für das Einspielen kritischer Patches
- Offline Backups
- Privileged Access Management
- Email Filtering & Validation Process, Phising Tests
- End of Life Software sollte ersetzt werden

Empfehlung in Bezug auf Ransomware Risiken:

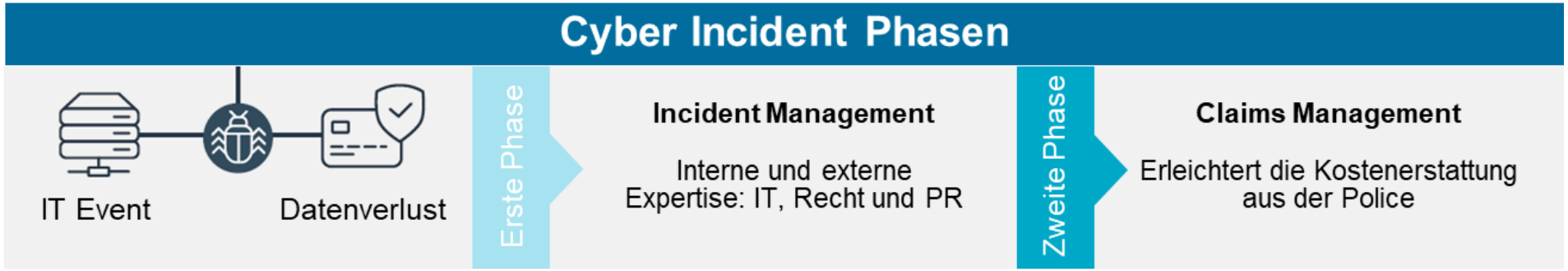
1. Stellen Sie sicher, dass angemessene Cybersicherheitskontrollen vorhanden sind.
2. Stellen Sie sicher, dass die Reaktionspläne auch Ransomware-Szenarien berücksichtigen und im Voraus getestet werden, inkl. der Einbindung von Dienstleistern.
3. Verstehen Sie die finanziellen Auswirkungen von Ransomware-Risiken und überprüfen Sie, ob ein Risikotransfer der Restrisiken sinnvoll ist.

Hinweis: Jeder Versicherer hat seine eigenen spezifischen Kontrollanforderungen, die sich je nach Umsatzgröße und Branchenklasse des Versicherten unterscheiden können

Versicherungsmarkt

Die wichtigsten Phasen nach einem Angriff

Im Schadenfall kommt es darauf an, von Anfang an die richtigen Maßnahmen zu ergreifen und das richtige Team an seiner Seite zu wissen.

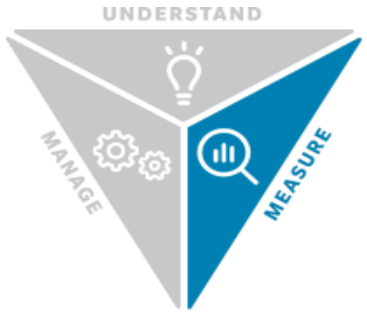


In der Praxis stellt jedoch gerade die Koordination der Maßnahmen und der externen Dienstleistungen eine große Herausforderung dar, für die sich in der Regel niemand verantwortlich fühlt. Eine Lösung könnte das Einsetzen eines „**Regisseurs**“ sein, der Teil des Versicherungsschutzes ist.

Zusammenfassung / Key take aways

Zusammenfassung/ Key Takeaways

- Lernen Sie Ihr Risiko genau kennen, nur so können Sie geeignete Gegen-maßnahmen treffen.
- Schaffen Sie Verantwortlichkeiten für den Bereich Informationssicherheit, die direkt an das Management berichten
- Vernetzen Sie sich mit Kollegen aus den relevanten Abteilungen (z.B. IT, Personal und dem Bereich Finanzen). Cyber ist kein reines IT-Thema!



- Quantifizieren Sie das Risiko: ein Schadenfall kann wesentlicher höher ausfallen, als Sie denken.
- Testen Sie regelmäßig Ihre technisch-organisatorischen Maßnahmen durch Pentrationstests oder Krisenstabsübungen.
- Überprüfen Sie mit Hilfe einer Deckungsanalyse, ob das nicht vermeidbare Restrisiko wirklich versichert oder versicherbar ist.

- „Pick the team before the game“
- Passen Sie Ihre Krisen- und Notfallpläne dem individuellen Cyber Risiko an.
- Awareness-Trainings für Mitarbeiter, Stichwort „Human Firewall“
- Erstellen Sie ein individualisiertes Versicherungskonzept.
- Wiederholen Sie den gesamten Prozess regelmäßig und testen Sie die Krisenpläne.

Kontakt

Dipl. Kfm. (FH) Ingo Gurcke, Geschäftsführer, Marsh Medical Consulting

Bismarckstraße 2| 32756 Detmold, Deutschland

+49 (0)5231 30819-110 | Mobil: +49 (0)152 01625-110

Ingo.gurcke@marsh.com

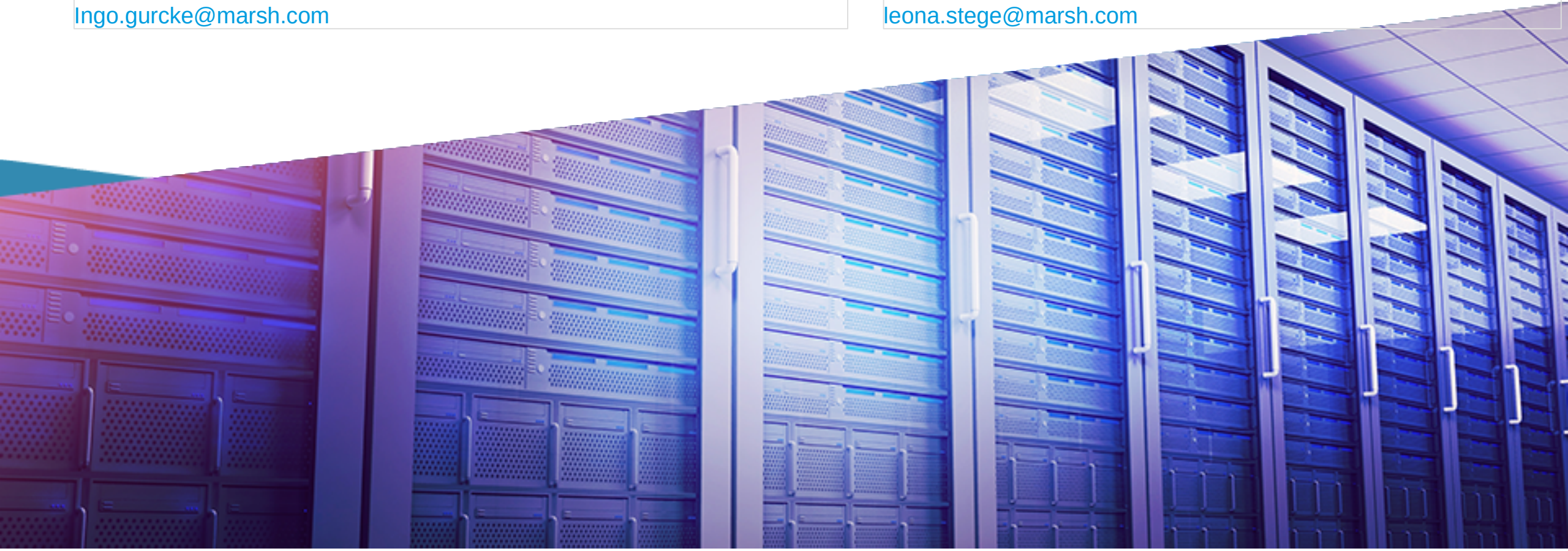
Kontakt

Leona Stege, Senior Fachbetreuerin, CYRIS

Brandstwiete 1 – Neuer Dovenhof | 20457 Hamburg, Deutschland

+49 (0)40 37692-256 | Mobil: +49 (0)152 01622-126

leona.stege@marsh.com



Marsh Medical Consulting

A business of Marsh McLennan