Information Security
in Healthcare

D: Brack, Principal Information Security

RANSOMWARE 360° – INFRASTRUKTURTEST UND CYBERSECURITY-AWARENESSPROGRAMM

T · · Systems · Let's power higher performance

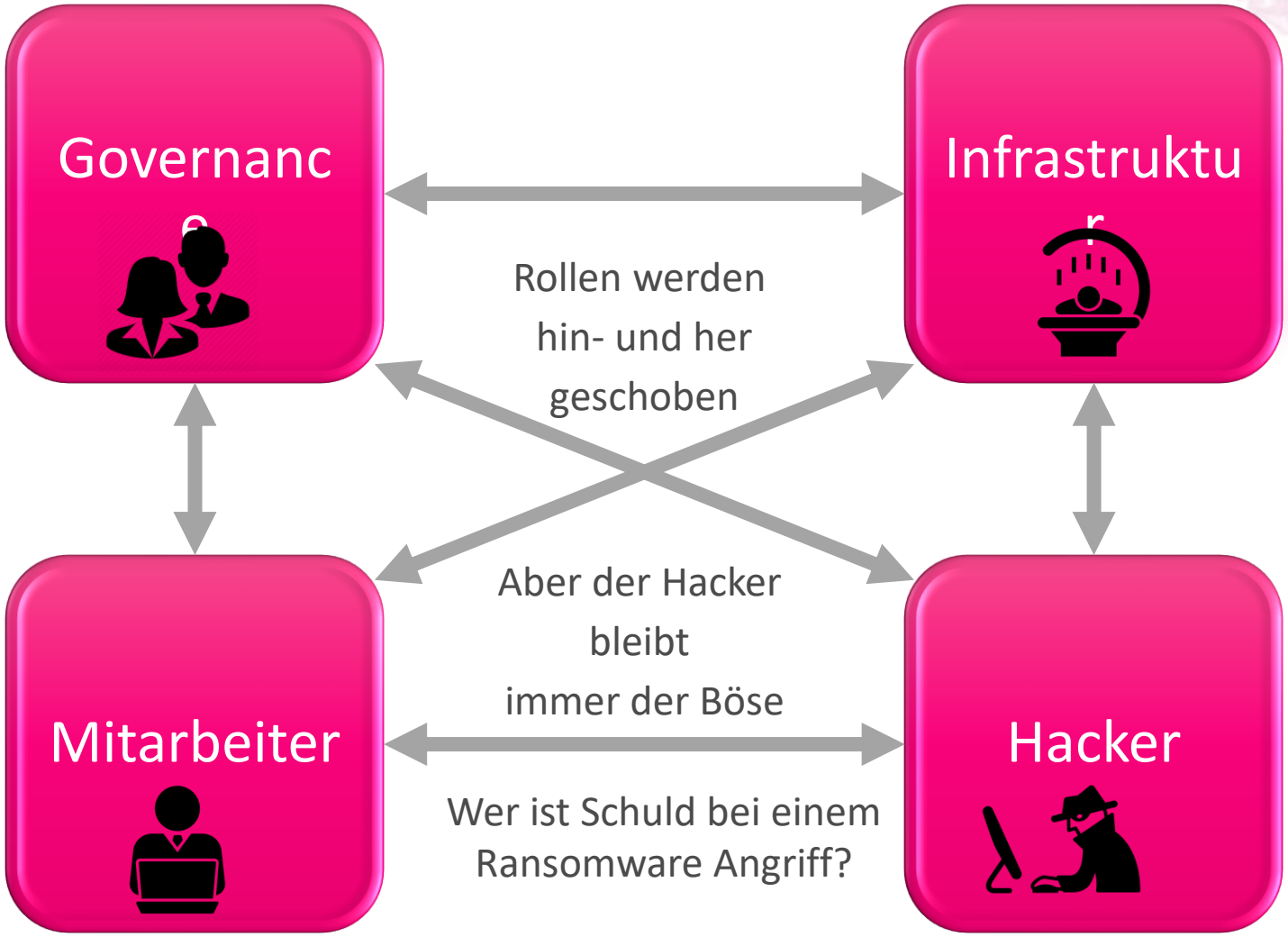
T-Systems: Die Spezialisten für Schafe im Wolfspelz oder Umgekehrt

Die Protogonisten (Die Keystakeholder im Ransomware Universum):

- Governance
- Infrastruktur
- Mitarbeiter
- Hacker

Das Dramaviereck?

Dramaviereck (Opfer, Retter, Verfolger, Profiteur)



Nach einem Ransomewareangriff..

- **Ich habe es ja immer gesagt**
- **Hättet Ihr auf mich gehört**
- **Wir investieren zu wenig**
- **Ist alles zu kompliziert**
- **Wir haben kein Budget**
- **Am falschen Ende gespart**
- **Die haben ja keine Ahnung**
- **Macht es einfach sicher**
- **Dies war euer Auftrag**
- **Wie soll ich das Wissen**
- **Wir haben ja Spezialisten**

Wer ist Schuld bei einem Ransomware Angriff?

Die Geschäftsleitung

Governance

Der Mensch

Mitarbeiter

Die Technik

Infrastruktur

Der Hacker

Hacker

Erhebung durch Händeheben

1. Rang
2. Rang
3. Rang
4. Rang

Wer ist Schuld bei einem Ransomware Angriff?

Die gute Nachricht:

Wir können ihnen zu jedem dieser Bereiche verschiedenste Lösungen anbieten.

Die schlechte Nachricht:

Auch das wird das Problem Ransomware nicht lösen.

Dramaviereck (Opfer, Retter, Verfolger, Profiteur)

Governanc
e

Mitarbeiter

Nach einem Ransomewareangriff..

ja immer gesagt

uf mich gehört

eren zu wenig

kompliziert

kein Budget

n Ende gespart

keine Ahnung

infach sicher

war euer Auftrag

- Wie soll ich das Wissen
- Wir haben ja Spezialisten

Das führt nicht zum Erfolg bei der Bekämpfung komplexer Cyber Angriffe.

Nur gemeinsam kann man Erfolgreich sein.

Ja sogar mit den Hackern kann/ muss man sich arrangieren.

Der Quick Fix

Ja leider..

Es muss miteinander geredet werden

Wie 3D-Druck die lebensrettende Operation eines komplexen Wirbelsäulensarkoms ermöglichte

Krisenbewältigung muss beübt werden.
Spitzenmedizin kann das ja eigentlich fast am besten, nebst Feuerwehr, Polizei und Militär.
Wieso kann dass den IT nicht?

Stiftung für Patientensicherheit – die bessere Strategie als IT Frameworks?

Ein von der Stiftung für Patientensicherheit durchgeführter Literaturreview zu Effektivität, Compliance und Erfolgsfaktoren bei der Implementierung chirurgischer Sicherheitschecklisten zeigt eine breite Wirksamkeit für das klinische Outcome.

Checkliste = Synonym für DR und BCM Pläne oder aber Playbooks für Restore, Backps und Archivierung.

Eine Checkliste ist – richtig eingesetzt – Hilfsmittel und Prozesselement zugleich. Sie dient nicht primär als klinische Entscheidungshilfe, sondern wirkt als Erinnerungs- und Entlastungsinstrument. Gerade Dinge und Handlungen, die an sich selbstverständlich sind, gehen in der klinischen Routine häufig unter. Checklisten können dabei helfen, dass das nicht passiert. Zudem ermöglichen sie eine klar strukturierte, auf das Wesentliche konzentrierte Kommunikation im Team. Dank der Sicherung der Abläufe durch Checklisten können sich Fachpersonen auf die komplexen Fragestellungen konzentrieren, die ihr spezifisches Fachwissen voraussetzen. Zudem erhalten sie Raum, ihre Aufmerksamkeit auf andere Informationen zu richten, die eine rechtzeitige Antizipation von kritischen Ereignissen ermöglichen.

https://www.patientensicherheit.ch/fileadmin/user_upload/1_Projekte_und_Programme/progress_sichere_chirurgie/progress_SC_alle/5_SR_5_Sichere_Chirurgie_D_160725.pdf

Governance bei Ransomware Attacken

- ✓ Cybersecurity strukturieren durch das einführen eines ISMS (ISO27701)
- ✓ CISO oder vCISO Einstellen
- ✓ Fachkräfte oder Berater Kontakte Pflegen
- ✓ Krisenstab bilden
- ✓ Regelmässige Übungen und Simulationen durchführendes
- ✓ Externes Audit zur Überprüfung der Sicherheit
- ✓ Cybersecurity gehört auf die Agenda der Geschäftsleitung mit Regelmässigen Reporten
- ✓ Outsourcing und externe Dienstleistungen auf Compliance überprüfen
- ✓ Zusammenarbeit der IT, Medizin IT und auch der OT inklusive der Compliance und Rechtsabteilung

Ergänzungen/ Erfahrungen aus dem Publikum Willkommen

Infrastruktur bei Ransomware Attacken

Infrastruktur

- ✓ Überprüfen der Infrastruktur in der Erfüllung der Mindestanforderungen
- ✓ Regelmässige Technologieupdates
- ✓ Regelmässiges Pentesting auf Netzwerk und Applikationsebene
- ✓ Überprüfen neuer Systeme und Applikationen vor der Inbetriebenahme
- ✓ Kontrolle der SLA's mit den Anbietern – erfüllen die SLAs die Mindeststandards?
- ✓ Segregation Zero Bsp. Trust Framework
- ✓ Grundschutz für die ganze Infrastruktur
- ✓ Fremdgeräte nicht vergessen (Snackautomaten, Parksysteme mit Remote Zugriff etc.)
- ✓ SIEM und / oder ein SOC nutzen
- ✓ Konsequentes Vulnenrability Management
- ✓ Pikett Organisation

Ergänzungen/ Erfahrungen aus dem Publikum Willkommen

Mitarbeiter bei Ransomware Attacken

- ✓ Bewusstsein der Mitarbeiter schärfen
- ✓ Awarenesschulungen
- ✓ Bei Unklarheiten nachfragen Helpdesk und oder CISO
- ✓ Sich gegenseitig absprechen – eine Kollegin oder einen Kollegen fragen
- ✓ Phishing Emails und Sicherheits- Vorfälle melden
- ✓ Regelmässigen Phishing Simulationen und Awareness Schulungen durchführen
- ✓ Achtsam sein

Ergänzungen/ Erfahrungen aus dem Publikum Willkommen

Governance bei Ransomware Attacken

- ✓ Klare Verhaltensregeln bei Ransomware Angriff
- ✓ Mit den Hackern Verhandeln (Zeitgewinn)
- ✓ Keine Zahlung durch ein GL- Mitglied
- ✓ Eine Dritt Partei beiziehen
- ✓ Fallbeispiele besprechen im Krisenstab
- ✓ Krisenstab Übung Anhand eines Ransomware Angriffs

Ergänzungen/ Erfahrungen aus dem Publikum Willkommen

Security Awareness

Das stärkste Glied in der Kette ist der

Mensch!

Wenn die Technik versagt bleibt nur noch der Mensch.

Ansonsten wird’s der CISO richten mit Awareness Schulungen.

Diskussion & Fragen

Wir sind für Sie da, Danke!

T · · Systems · Let's power higher performance