SUMMARY DER LEARNINGS

«Wie ein Schweizer KMU ohne Lösegeld, dafür mit Militärtaktik einen Hackerangriff überlebt hat.»
NZZ; 10.7.2019

Martin Kelterborn
CEO OFFiX Holding AG

Learnings

GESCHWINDIGKEIT

Aussage:
Wir haben viel zu langsam reagiert…46 Stunden bis zum Shut down.
Erkenntnis:
Wir waren uns zu lange nicht bewusst, dass wir angegriffen wurden und die IT hoffte, es selber zu flicken
Konsequenz:
Es muss ein Standardprozess geben, der das Abschalten der Systeme unabhängiger von menschlichem Ermessen macht

VERTRAUEN IN DIE EIGENE IT

Aussage:
Interne rund auch externe Fachleute haben uns eine gute IT Sicherheit zugestanden
Erkenntnis:
Fachleute ist ein relativer Begriff für diese neue Bedrohung
Konsequenz:
Simulationsangriffe ausführen, durch unabhängigen Partner

KOMMUNIKATION INTERN

Aussage:
Die MA brauchen verständliche Infos, emotionale Begleitung und Präsenz des Chefs
Erkenntnis:
Führunsg-Rhythmus, Symbole, klare (Bild)-Sprache
Konsequenz:
Kommunikation bleibt Chefsache, das kann man nicht dem IT Chef delegieren

IT

Aussage:
Wir waren der Meinung, eine gute IT Sicherheit zu haben
Erkenntnis:
Wir haben sehr effizient, eine suboptimale IT-Architektur betrieben
Konsequenz:
Back-ups wieder physisch trennen...wie früher

MITARBEITER SENSIBILISIERUNG

- Dauerjob: Vom 1. Arbeitsvertrag bis zur Pension
- Anlaufstelle – Notfalltelefon
- Bring-Schuld der GL
- Remember May 17.day

RESSOURCEN

Aussage:
Die bestehenden personellen Ressourcen funktionieren 36 Stunden und sind tw. überfordert
Erkenntnis:
Keine Hemmungen Ressourcen ins System zu pumpen
Konsequenz:
Adressen und Bezugspersonen in Friedenszeiten kennen

FÜHRUNG CEO

Aussage:
Ich wäre am liebsten selber in den Schützengraben gestiegen
Erkenntnis:
CEO koordiniert, was bisweilen unbefriedigend ist
Konsequenz:
Nicht stören, aushalten und vorbehaltene Entschlüsse treffen

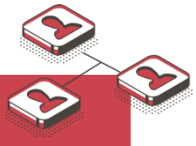
FÜHRUNG ALLGEMEIN

Aussage:
Ob eine Führungscrew funktioniert, zeigt sich in der Krise
Erkenntnis:
In Friedenszeiten keine Rücksicht nehmen
Konsequenz:
Keine Kompromisse bei Chefposten va. was die Persönlichkeit betrifft.
Persönlichkeit schlägt Leistungsausweis

HABEN SIE GEWUSST, DASS….

- Ein Passwort immer 2 Mal geändert werden muss
- Gelöscht ist nicht gelöscht
- Zurückgesetzt ist nicht zurückgesetzt
- Abgestellt ist nicht abgestellt

….ANSONSTEN FRAGEN SIE IHREN CYBER CRIME SPEZIALISTEN!



ORGANISATORISCHES

- SIBE IT Sicherheit ernennen
- IT Know-How im Verwaltungsrat

Schlussfragen

Welche Kompetenzen hat ihr IT Chef im Bereich Cyber Crime?

Welche Kompetenzen im Cyber Crime hat Ihr externe IT Partner? Wie lange (in Stunden) kann der für Sie arbeiten?

Wen rufen Sie an, wenn Sie Hilfe brauchen?

Wie oft thematisieren Sie das Thema in der Geschäftsleitung?

Und last but not least, haben Sie dafür gesorgt, dass Ihre Mitarbeiter in der Erkennung von Cyber Crime kompetenter werden?