Hackerangriff in Aerzen

AERZEN
EXPECT PERFORMANCE

Hackerangriff in Aerzen

Agenda

1. Kurzvorstellung Aerzener Maschinenfabrik
2. Der Angriff und seine Auswirkungen
3. Gegenmaßnahmen
4. Zukunftsausrichtung

AERZEN
EXPECT PERFORMANCE

1. AERZEN – Allgemeine Informationen

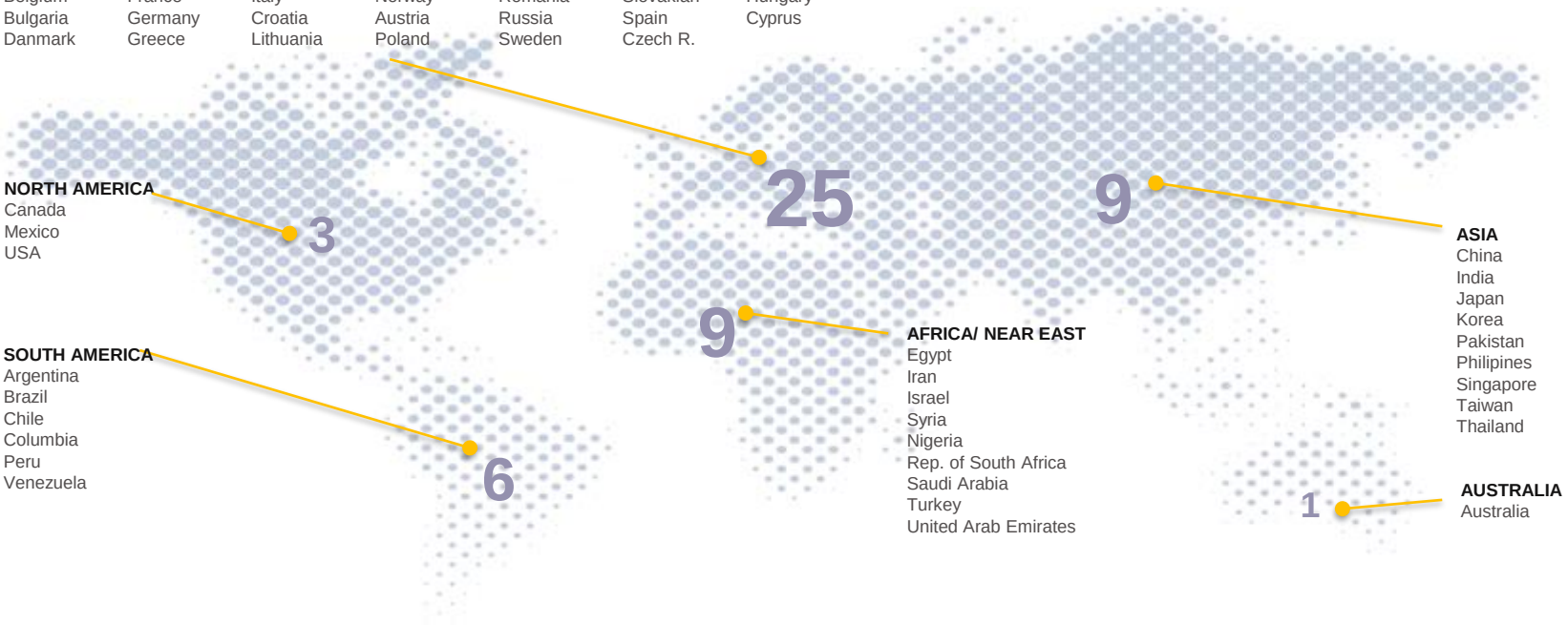
AERZEN
EXPECT PERFORMANCE

Allgemeine Informationen

- Gründung: 1864
- Mitarbeiter (Stammhaus): ca. 1.100
- Tochtergesell-schaften: > 50
- Mitabeiter (international): ca. 1.500
- Umsatz: 450 Mio. € (Gruppe)
- Geschäftsführung: Klaus-Peter Glöckner
Björn Irtel
- Aufsichtsrat: Klaus-Hasso Heller

AERZEN
EXPECT PERFORMANCE

AERZEN – überall eine gute Adresse!



AERZEN
EXPECT PERFORMANCE

AERZEN Produkt Program

Drehkolben-gebläse

Delta Blower

Gebläse für Über- und Unterdruck

Vakuumgebläse

Prozessgas Gebläse

Biogas Gebläse

Turbogebläse

Aerzen Turbo

Schraubenverdichter

Delta Screw

Schraubenverdichter ölfrei

Schraubenverdichter öleingespritzt

Scharubenverdichter für Prozessgas und Biogas

Drehkolben-verdichter

Delta Hybrid

AERZEN
EXPECT PERFORMANCE

Anwendungsgebiete für AERZEN Produkte

- Pneumatischer Transport
- Chemie- und Verfahrentechnik
- Umweltschultz *(z. B. Kläranlagen)*
- Kraftwerkstechnik
- Petrochemie
- Drucklufttechnik
- Hochvakuum
- Kälteindustrie
- Öl- und Gastechnik
- Stahlproduktion
- Trinkwasser Aufbereitung
- Glasherstellung
- Lebensmitteltechnik
- Bergbau
- Und viele andere …

… überall, wo Gase gefördert oder verdichtet werden!

Pneumatischer Transport

Abwassertechnik

AERZEN
EXPECT PERFORMANCE

2. Der Angriff und seine Auswirkungen

AERZEN
EXPECT PERFORMANCE

Der Angriff und seine Auswirkungen

- 28.07.2021: Hackerangriff mittels Schadsoftware
- Alle Systeme wurden vorsorglich heruntergefahren, alle Geschäfts-prozesse kamen zum Erliegen (Mail, Telefon, Produktion …)
- Diverse Systeme und Server waren kompromittiert (im Stammhaus und in den deutschen Vertriebsbüros), erfreulicherweise nicht das zentrale SAP-System allerdings auch Bearbeitungsmaschinen und Lagersysteme
- Erpressungsversuch, aber keinerlei Verhandlungen (Darknet/TOR Browser)

AERZEN
EXPECT PERFORMANCE

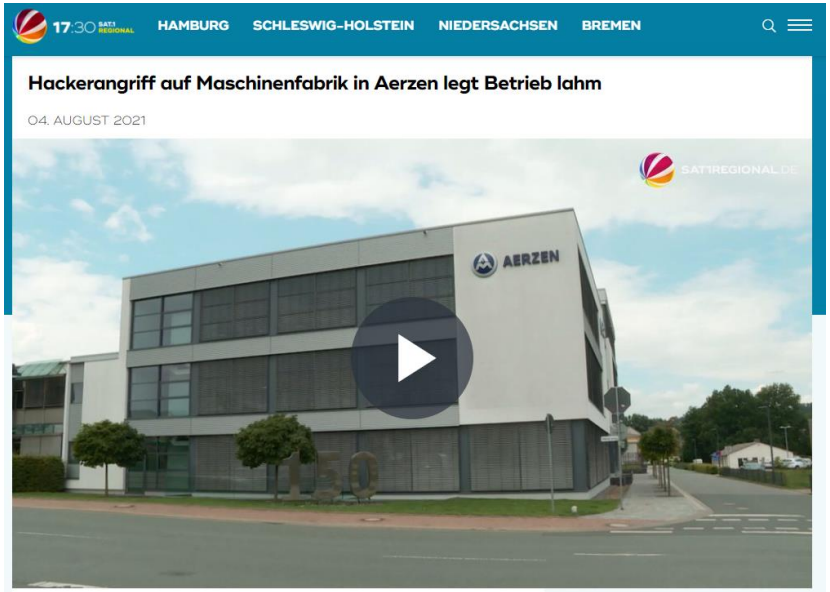
Der Angriff und seine Auswirkungen

- Alle Geschäftsprozesse kamen zum Erliegen, u. a.:
  - keine Produktion, keine Lieferungen!
  - kein Wareneingang!
  - keine interne Logistik, keine Auslagerungen!
  - keine Kommunikationsmöglich-keiten! Nur Mobiltelefonie!
  - die Website wurde ebenfalls lahmgelegt
  - Manueller Zahlungsverkehr!
  - Nur Papier und Stift!
- Alle Mitarbeiter (außer IT) mussten in den Zwangsurlaub

AERZEN
EXPECT PERFORMANCE

Der Angriff und seine Auswirkungen

- „Belagerung“ durch die Presse
  - lokale Zeitung
  - lokale und überregionale Radiosender
  - lokale und überregionale Fernsehsender
- der Wettbewerb versuchte, die Situation entsprechend auszunutzen
- In den Monaten August/September konnte kaum Umsatz generiert werden



AERZEN
EXPECT PERFORMANCE

3. Gegenmaßnahmen

AERZEN
EXPECT PERFORMANCE

Gegenmaßnahmen – wie sind wir vorgegangen?

- Gründung einer Task Force:
  Abstimmung 3x am Tag
- Aufbau neuer Kommunikationskanäle (Messenger Dienste) für Auslandsgesellschaften und Führungs-kräfte/Mitarbeiter: tägliche Mitteilungen
- Aktive Beteiligung des Betriebsrates
- Stopp der Kommunikation an die Presse
- Meldung an die Behörden:
  - Datenschutzbeauftragter AERZEN
  - Landesdatenschutzbeauftrage Nieders. (LDS)
  - Polizei (LKA->BKA->FBI) Strafanzeige
  - BSI „Meldung ohne Folgeaktivitäten“

Teambuilding

AERZEN
EXPECT PERFORMANCE

Gegenmaßnahmen – wie sind wir vorgegangen?

Priorisierung von Fachbereichen

1. Logistik und Versand
2. Service
3. Produktion im Bereich Standardmaschinen

- ✓ Nach 3 Tagen konnte die Telefonzentrale wieder Inbetrieb gehen
- ✓ nach 1 Woche konnten wieder dringende Lieferungen vorgenommen werden
- ✓ Nach 6 Wochen waren Logistik und Service wieder arbeitsfähig
- ✓ Nach 8 Wochen startete die Produktion in priorisierten Bereichen

AERZEN
EXPECT PERFORMANCE

Gegenmaßnahmen – wie sind wir vorgegangen?

Kompletter Neuaufbau der IT Infrastruktur (Weltweit)

- Einbindung von externen Spezialisten (u.a. Forensik)
- Internationaler Support/Consulting
- Unterstützung der IT mit internen Kräften aus vielen Fachbereichen
- 24/7 Dienst über 12 Wochen
- Mehr als 4500 Überstunden in der IT
- RED Field -> Orange Net (Quarantäne) -> Green Field
- Wiederherstellung der Systeme/Daten (BackUp)!!
- …

AERZEN
EXPECT PERFORMANCE

4. Zukunftsausrichtung

AERZEN
EXPECT PERFORMANCE

Zukunftsausrichtung

IT-Infrastruktur/Maßnahmen/Organisation

- Neue IT-Infrastruktur weltweit (Netzwerktopologie,…)
- SOC/MDR
  MFA, …
- Angepasste und weltweit vereinheitlichte Sicherheitskonzepte/Richtlinien
- Hohes IT Investitionsbudget in 2022
- Versicherung
- IT-Security
- 100% Sicherheit? NEIN

AERZEN
EXPECT PERFORMANCE

CYBERKRIEG (FAZ 03. April 2022)

Amerika warnt vor groß angelegten russischen Hackerangriffen. Das sollte man ernst nehmen. Auf dem virtuellen Feld haben die Russen schon oft gezeigt, was sie können.

Wenn die Amerikaner vor einem Angriff warnen, sollte die Welt aufhorchen …

YBERKRIEG

Amerika warnt vor groß angelegten russischen Hackerangriffen. Das sollte man ernst nehmen. Auf dem virtuellen Schlachtfeld haben die Russen schon oft gezeigt, was sie können.

Von Morten Freidel

EXPECT PERFORMANCE.

WORKING TOGETHER FOR A MORE EFFICIENT WORLD!

AERZEN
EXPECT PERFORMANCE