Cyber Security in der praktischen Umsetzung

Was uns eine Swisscom Rechnung gelehrt hat

Christian Eckert, CEO Regloplas AG

REGLOPLAS

Temperiertechnik

Technologien

Druckguss (Aluminium)
Spritzguss (Kunststoff)
Extrusion

Märkte

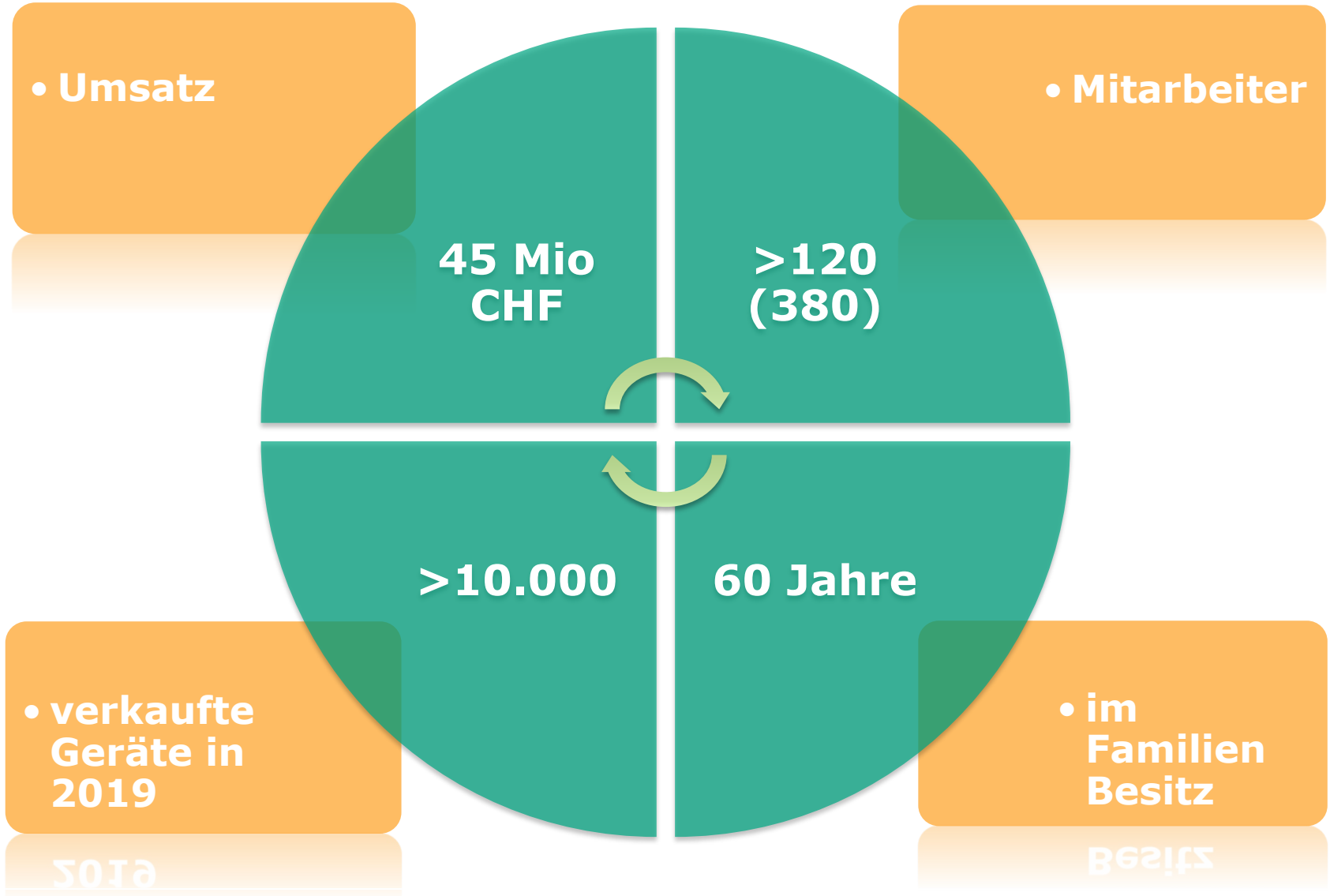
Automobil
Medizin
Food
Raumfahrt
Elektronik

REGLOPLAS

REGLOPLAS AG

Unternehmen

Facts & Figures



REGLOPLAS

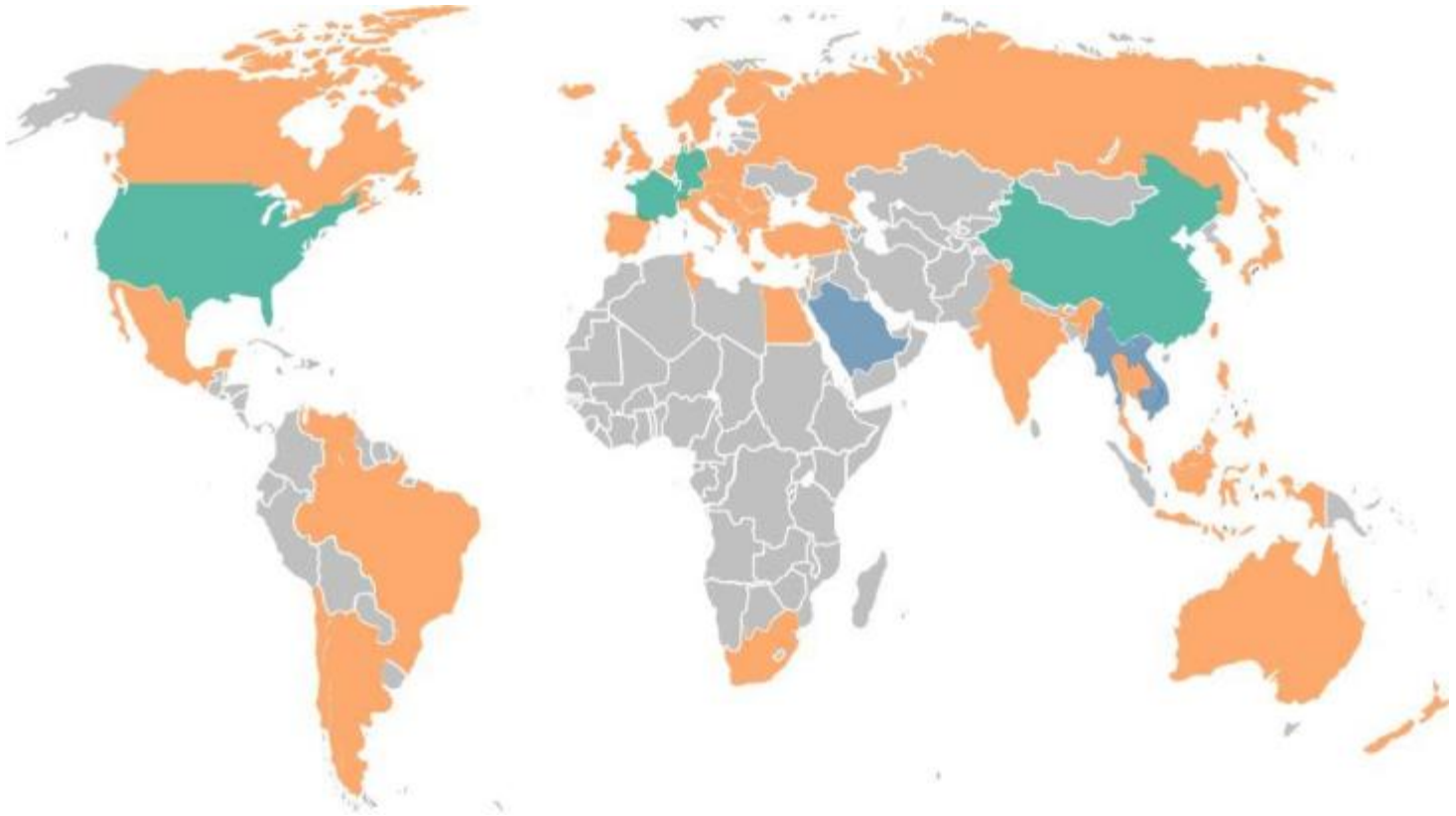
Niederlassungen

Partner

Aktueller Marktausbau

REGLOPLAS

Weltweites Verkaufs- und Servicenetzwerk



REGLOPLAS

REGLOPLAS AG

Software & Hardware

(vor dem Vorfall)

1. Installation der Server in house
2. ERP, CRM, 3D Cad, Elektro CAD, PPS, Buchhaltung etc.
3. Tägliche Backups
4. Offline Zahlungssystem mit Zweifachunterschrift
5. Externe Systembetreuung
6. Kontinuierliche Erneuerung der Hardware
7. Regelmässige Updates

➔ Sicheres System

REGLOPLAS

REGLOPLAS AG

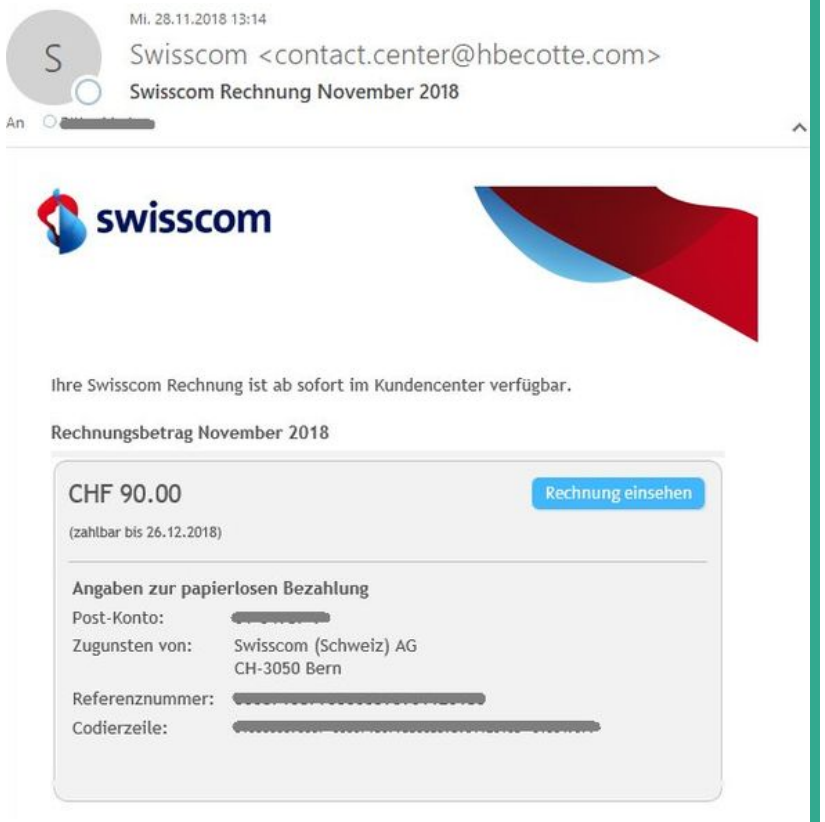
Grundsolides KMU

Urs Zeller, Rechnungswesen

REGLOPLAS

Was ist geschehen?

REGLOPLAS



Vor dem Ereignis

- Auf dem PC von Herrn Zeller Swisscom-Email eingegangen
- Durch Klick auf «Rechnung einsehen» wurde Dridex installiert
- Dridex spioniert Informationen von Offline Zahlungssoftware

03.04.2017 nach 17:00

- Dridex löst Zahlungen bei den Banken aus

04.04.2017 um 02:00

- Täterschaft startet DOS Attacke auf Regloplas AG, Ziel System von Regloplas AG für den 04.04.2017 lahmlegen, damit Zahlungen nicht auffallen, Swisscom stellt Internetzugang automatisch ab

➔ Nur die zufällige Entdeckung der Zahlungen am Vorabend hat grösseren Schaden verhindert!!!

REGLOPLAS

03. April 2017

- 19:00, Anruf Herr Zeller, Frage: Hast Du Zahlungen über 1’200’000.– CHF ausgelöst?
- Analyse der Zahlungsaufträge

USD 196'750.10	Rechtsanwalt Deutschland
GBP 35'829.90	Gebäudefirma England
GBP 36'129.93	Gebäudefirma England
EUR 96'728.57	Metallfirma Rumänien
EUR 258'613.90	Trading Hong Kong
EUR 268'525.79	Unbekannt Belgien
EUR 46'770.95	Service Unternehmen Portugal
EUR 49'284.60	Gebäudefirma England

- Sämtliche Firmen sind uns nicht bekannt
- Meldung an Banken mit der Aufforderung sämtliche Zahlungen zu stoppen
- Banken senden SWIFT an Empfängerbanken um Auszahlungen zu stoppen, sämtliche Konten sind gesperrt

REGLOPLAS

04. April 2017

06:30 Eintreffen Regloplas AG
06:45 Sämtliche internen Netzwerke sind überlastet
08:00 Regloplas AG wird mit einer DOS Attacke angegriffen
08:15 Netz nach aussen wird abgeschaltet
09:00 Entscheid Reboot Systeme mit Stand 02. April 2017

➔ Kein normaler Betrieb möglich

09:30 Kriminalpolizei Anzeige erstatten
10:00 Start Untersuchung PC's auf Dridex Programm
20:00 Keine Neuigkeiten von den Banken
21:00 4 PC's sind mit Dridex infiziert

Status: 1'200'000.- CHF Verlust, kein Betrieb möglich

REGLOPLAS

05. April 2017

08:00 Start aller Systeme auf Stand 02. April 2017
14:00 Mitarbeiter können wieder relativ normal arbeiten
16:00 Meldung: «kleinere» Beträge in England mit Kreditkarten abgehoben bevor Banken öffneten

Status: 1’200’000.- CHF Verlust, Betrieb eingeschränkt möglich

06. April 2017

16:00 Meldung das einzelne Zahlungen gestoppt wurden
17:00 Rückvergütungen aller grossen Beträge eingegangen

Status: 160’000.- CHF Verlust, Betrieb uneingeschränkt möglich

05. Januar 2019

15:00 Meldung Staatsanwaltschaft, Interpool konnte in Litauen 50’000.- CHF sicherstellen

Status: 110’000.- CHF Verlust, Betrieb sicherer!

REGLOPLAS

Wir sind mit einem blauen Auge davongekommen

REGLOPLAS

REGLOPLAS AG

Learnings

- Zahlungen über vermeindlich sichere Offline-Zahlungssysteme werden von Banken nicht überprüft, keine Sicherheit

  ➔ Zahlungsfiles nur noch über Internetbanking auslösen

- Spionagesoftware durch Email erhalten, kein Schutz durch Virensoftware / Firewall

  ➔ Installation Zahlungs-PC mit eigenem Betriebssystem, über 4G vernetzt ins Internet, kein Outlook

- Täterschaft braucht Zeit um an alle Informationen zu gelangen

  ➔ Regelmässige Passwortänderung

Mit wenig Aufwand grosse Sicherheit

REGLOPLAS

REGLOPLAS AG

Software & Hardware

(heute)

1. Installation neues ERP, CRM, PPS etc. in Amazon Cloud
   - kontinuierliche Updates durch Serviceprovider
   - always on System (gespiegelte Daten auf mind. 3 Servern)

2. 3D Cad, Elektro CAD auf inhouse Servern
   - tägliche Backups
   - Test der Backups

3. Sämtliche Officeanwendungen Office 365
   - Daten in Cloud / Sharepoint
   - Lokaler Backup der Clouddaten

4. Drei unterschiedliche Internetprovider mit mehreren Zuleitungen inkl. 5G

5. Einführung zentrales Software-deployment-System; locale Clients mit stark eingeschränkten Rechten

6. Serverupdates in definierten Abständen

7. Kontinuierliche Sicherheitsüberprüfung durch Dritte

➔ Sicheres System, ausser wenn kein Internet vorhanden

REGLOPLAS

Besten Dank

REGLOPLAS