CYBER SECURITY & COVID ZEIT

www.suntis.ch

SUNTIS AG | Viale Stazione 13| CH-6500 Bellinzona | info@suntis.ch | +41 91 821 8000

SUNTIS in Kürze

- Seit 1999 wird SUNTIS von führenden Telekom-, Service-, Versorgungs- und Transportanbietern als vertrauenswürdiger Partner einbezogen, um anspruchsvolle ICT Lösungen zu realisieren.

- Wir decken alle ICT Prozesse, von Anforderungen bis zur Inbetriebnahme.

- ICT Partner:
  - Artificial Intelligence
  - Blockchain
  - 5G, IoT, eSIM

- Wir entwickeln kundenspezifische Lösungen und liefern Systeme basierend auf unseren OSS / BSS Produkten SUSI und SNOW in Bereichen:
  - IoT-, Rail-, Utility-, Telekom und MVNO.

SUNTIS in Kürze

- Mission

  OSS / BSS PRODUKTE:
  ✓ SNOW - Remote Smart Card Management
  ✓ SUSI - Lösungen für profesionelle Anwendung
  ✓ Security Produkte: SUNPAS (2FA), eLearning, PCI-Gateway, usw.

  LÖSUNGEN - Entwicklung von Lösungen für ICT-Kunden
  ✓ Digitalisierung, Cybersecurity, eLearning, ICT Lösungen

- Meilensteine

  ✓ 1988 Ascom Infrasys AG - Geschäftsstelle Bellinzona
  ✓ 1999 SUNTIS AG gegründet

- Hauptsitz — Viale Stazione 13, Bellinzona / Stützpunkte: Hong Kong, Süd Afrika
- Personal — Informatiker, Elektroingenieure & Informatik Lehrlinge.
- Management — Bruno Pini (CEO, VR), Orest Goricanec (CTO, VR), Max Gerber (CFO)
- Outsourcing — Zusammenarbeit mit lokalen und ausgewählten Partnern weltweit

Agenda 15.OKT.2020

1. CYBERKRIMINALITÄT
2. FALLBEISPIEL – 2FA & IoT
3. FALLBEISPIEL – SCHULUNG & SENSIBILISIERUNG

European Cyber Security Organisation (ECSO) Umfrage

Erkenntnisse der Umfrage von ECSO in Zusammenhang mit COVID in der Cybersecurity Gemeinschaft (März bis Mai 2020)

- Zunahme von Betrugsdelikten, Cyberkriminalität und Cyberangriffen.
- Die eingeschränkte Kapazität von aus der Ferne erbrachten Diensten und das mangelnde Vertrauen in die Remote-Datensicherheit.
- Legale Aspekte, Sensibilisierung, Cyber Schutzmassnahmen und Investitionen in Cybersecurity müssen während und nach der COVID Krise angegangen werden.
- **Artificial Intelligence**, **5G** und **IoT** sind die Technologien welche die Zukunft am meisten prägen werden.

Telearbeit und die Herausforderungen

Während COVID, hat Telearbeit stark an Bedeutung zugenommen.

Einige Herausforderungen, welche die Unternehmen beschäftigen:

- Sind die Mitarbeiter für steigende Cyberkriminalität gewappnet?
- Abhängigkeit Fernzugriffstechnologien, wie VPN (Virtual Private Networks).
- Potenzielle Gefahren zwischen beruflichen und privaten Geräten.
- Grössere Angriffsfläche, das interne Firmennetzwerk ist für mehr Mitarbeiter von aussen erreichbar.

Einige Daten

Gemäss Microsoft,

belaufen sich die Kosten der Cyber Kriminalität weltweit auf unglaubliche

$500 Milliarden

jedes Datenleck kostet eine Firma durchschnittlicher Grösse, ungefähr

$3.8 Millionen

63% aller Netzwerk Intrusionen und Datenklau sind die Folge von gestohlenen Benutzer Zugangsdaten

Gemäss einer Studie der Universität Erlangen-Nürnberg, behaupten viele Email Nutzer ie Cyber Risiken zu kennen und trotzdem bedienen viele die Links in empfangenen E-Mails

78 Prozent aller Email Nutzer behaupten die Risiken verbunden mit Anwählen unbekannter Links in E-Mails

Hackerangriffe erfolgen zunehmend über Emails. Gemäss Schätzungen beinhaltet eines von 131 Emails Malware. Erwartungen zufolge wird diese Zahl in Zukunft zunehmen, denn Hacker Benützen diese Mechanismen um ahnungslose Nutzer zu erpressen

1 von 131 Emails enthalten Malware

Cyberkriminalität – Hacker Profile

HOBBY HACKER

- Ruhm
- Beschränkte technische Möglichkeiten
- Sehr kompetent
- Veröffentlicht Erfolge

KRIMINELLE

- Vandalismus
- Beschränkte technische Möglichkeiten
- Alleine oder in kleinen Gruppen

HACKTIVIST

- Politische, soziale Motivation
- Entschlossen
- Alleine oder in Gruppen organisiert
- Sehr kompetent
- Weltweite Präsenz
- Gezielte Angriffe
- Veröffentlicht Erfolge

ORGANISIERTES VERBRECHEN

- Erpresser
- Geldwäscherei
- Betrug
- Professionell organisierte Banden
- Sehr kompetent
- Weltweite Präsenz
- Bedeutende finanzielle Mittel
- Malware
- Phishing Emails
- Adware
- IP Diebstahl

STAAT

- Politisch und industrielle Angriffe
- Sabotage
- Cyber Krieg
- Nationale Sicherheit
- Geheimdienst Organisationen
- Grosse finanzielle Mittel
- Sehr kompetent
- Angriffe gegen Institutionen
- Beeinflussung öffentlicher Meinung
- Cyber Terrorismus

ZUNEHMENDE RAFFINESSE und VERFÜGBARE RESSOURCEN

Cyber Sicherheit

Infrastruktur	Die IT Infrastruktur absichern (Anti-Virus, Firewalls) Zugangssicherheit verbessern (2-Faktor Authentisierung) Security Itelligence und Analytische Werkzeuge einsetzen
Sicherheits-Plan	Sicherheitsvorschriften erarbeiten Krisenmanagement vorbereiten Reaktion auf Angriff planen Überwachen und Identifizieren
Menschen	Der Mensch ist das schwächste Glied in der Abwehrkette Sensibilisierung durch Schulung Das Topmanagement einbeziehen Alle Mitarbeiter erreichen

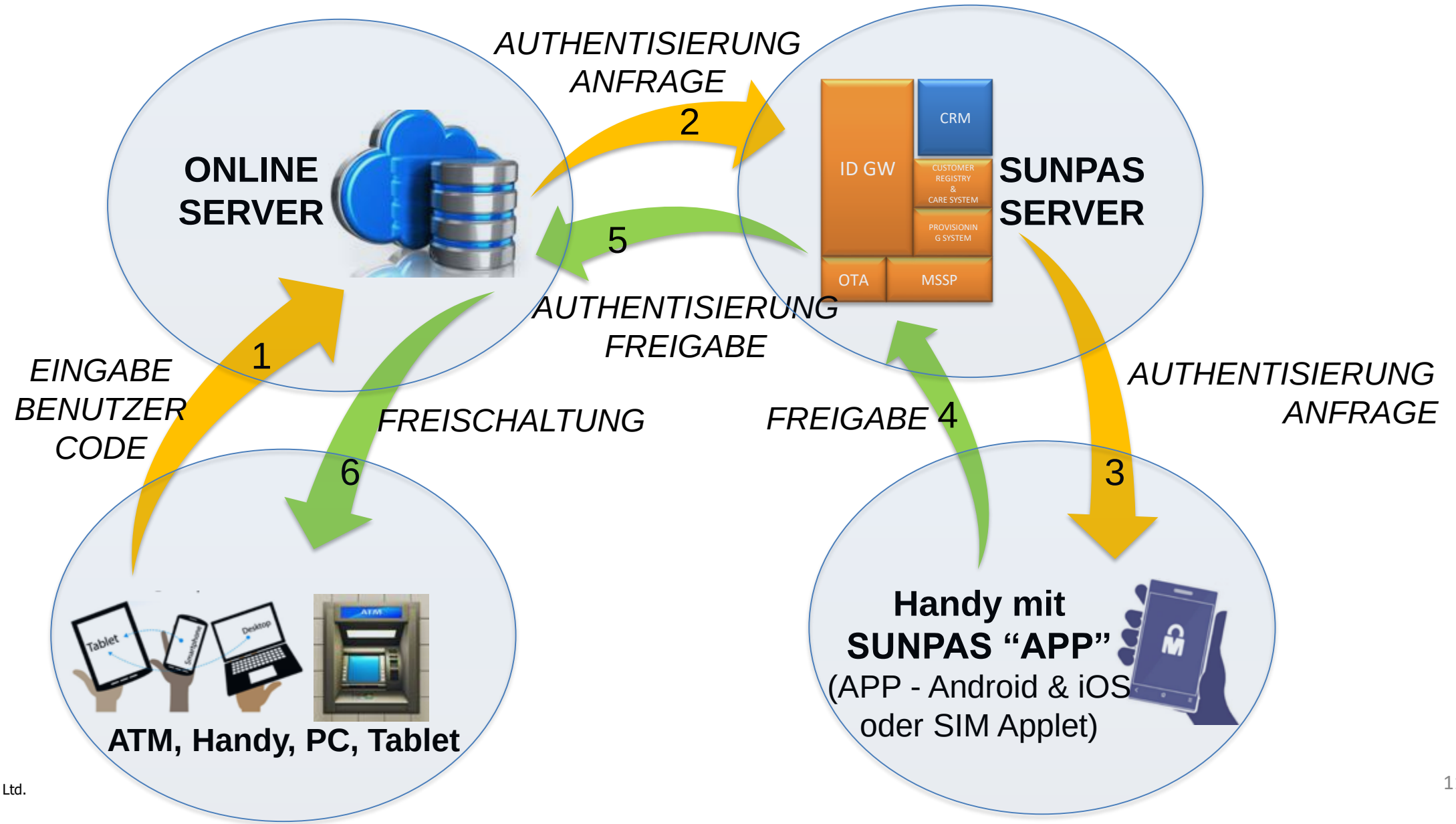
Source: Hueya, Inc. 2017

Authentisierung

- Digitale Online Dienste benötigen Benutzernamen, Passwörter und / oder weitere Codes (TAN) für eine gesicherte Anmeldung und Identifizierung

- Aber!
  - Mit der explodierender Anzahl von online Konti, ist es immer schwieriger sich an alle Benutzernamen und Passwörter zu erinnern
  - Sicherheitsprobleme nehmen zu
  - Es ist zunehmend schwierig die digitale Identität nachzuvollziehen
  - Immer häufiger sind Betrug und Verlust von Daten die Folge

SUNPAS – Zwei Faktor Authentisierung (2FA)

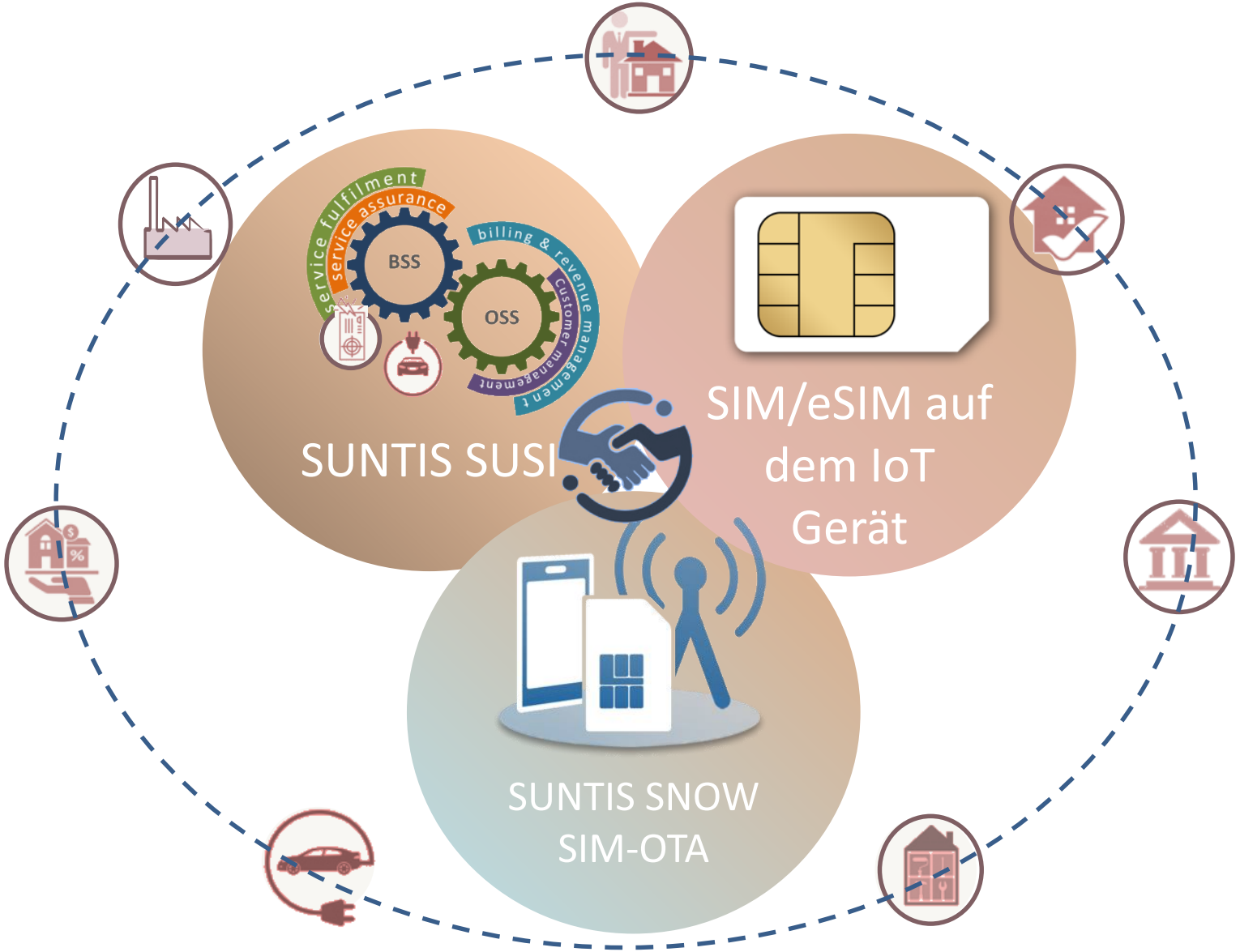


SUNPAS – Zwei Faktor Authentisierung (2FA) - Vorteile

- SUNPAS basiert auf dem GSMA Standard - Mobile Connect.
- Die Anmeldeprozedur für den Kunden ist wesentlich vereinfacht, lästige PINs werden nicht mehr gebraucht.
- Zum Handy hat nur der Kunde Zugang!

- Die Freigabe am Terminal ist von aussen nicht einsehbar.
- Wo keine Datenverbindung möglich ist, wird OTP eingesetzt.
- Kundendaten bleiben in der Schweiz!

IoT und Sicherung der Daten



LÖSUNGEN

	ZIELPUBLIKUM	METHODIK	RESULTATE
GUTACHTEN	• Alle Personen innerhalb einer Organisation	• Mitarbeiter werden für die Gutachtung ausgewählt • Mitarbeiter nehmen an der Online Gutachtung teil • Plattform befindet sich in Zürich	• Resultate werden zusammengefasst und mit dem Management abgestimmt um die weiteren Schritte zu definieren
SCHULUNG	• Management • Mitarbeiter, aufgeteilt in kleinere Gruppen • Maximum 15 Teilnehmer	• Schulung wird in Klassenzimmern durchgeführt • Dauer ca. 2 Stunden • Die Schulung wird Kundenspezifisch vorbereitet	• Resultate werden erstellt und dem Management zu Verfügung gestellt
eLEARNING	• Grosse Anzahl Personen, Anzahl unbeschränkt	• Auf 12 Sessionen verteilt (1xMonat) • Dauer einer Session -> 5 Min. • Anschliessend erfolgt ein Quiz • Die Plattform befindet sich in Zürich, Schweiz	• Resultate und Reports werden automatisch erstellt und verteilt
LÖSUNGEN	• Unternehmen mit hohen Sicherheitsanforderungen	• SUNTIS erarbeitet und entwickelt Lösungen um bei den bestehenden Legacy Systemen die Sicherheit entscheidend zu verbessern	• PCI DSS Lösungen • 2 Faktor Authentisierung • Vulnerability Assessment & Penetration Testing • Weitere...

Schulung & Sensibilisierung

- Ziel der Schulung ist das Bewusstsein und die Wahrnehmung der Cybersecurity Gefahren bei den Personen zu stärken und Schutzmechanismen akquirieren.

- Besuchen Sie unsere eLearning WEB Seite www.atelerix.ch

DANKE … FRAGEN?

Orest Goricanec

SUNTIS AG
Viale Stazione 13
CH-6500 Bellinzona
Switzerland

+41 79 444 0701
orest.goricanec@suntis.ch