

The art of creating time

Inhaltsübersicht

1. Motivation Cybercrime
2. Managed Security Services für Galexis (Referenzcase)
3. Vorstellung UMB
4. Fazit



Motivation Cybercrime



**Mit umfassender Cyber Security
die Geschäftsverfügbarkeit
sicherstellen**



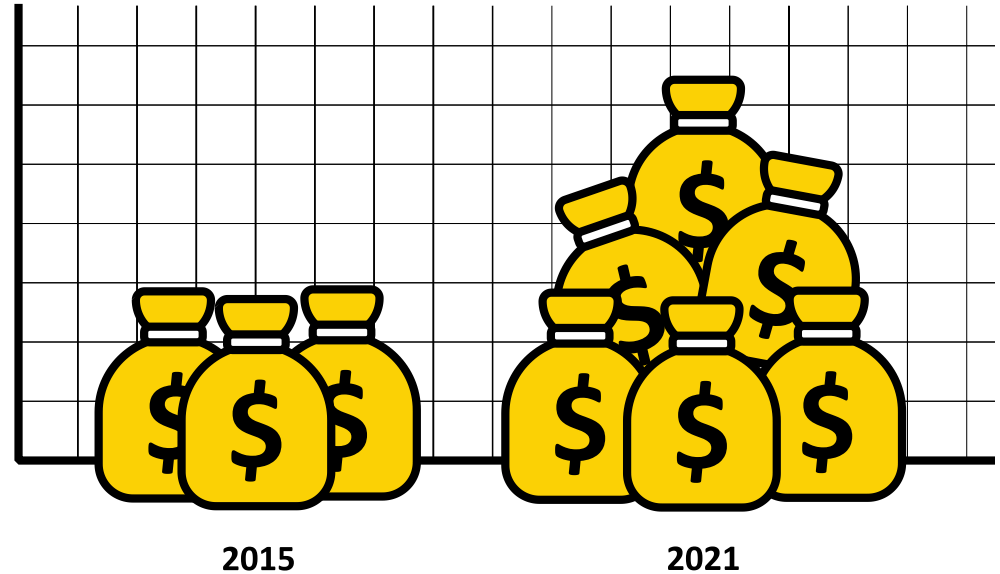
Schadensvorhersage

2021

- Cybercrime USD 6 Billionen
- Ransomware USD 20 Mia

2015

- Cybercrime USD 3 Billionen
- Ransomware USD 325 Mio



Anmerkung:

Profitabler als der weltweite illegale Drogenhandel!



Data Breach Statistiken

- Durchschnittliche Kosten pro Breach (mit IR Team) USD 3.86 Mio
- Höchste Kosten pro Breach USD 7.13 Mio (Healthcare)
- Durchschnittliche Kosteneinsparungen pro Breach mit einem IR Team USD 2Mio
- Betroffenste Industrie Healthcare
- Durchschnittliche Entdeckungsdauer (Healthcare) 280 Tage
329 Tage
- Kompromitierte Datensätze 80% Kunden (persönlich identifizierbare Informationen)
32% Geistiges Eigentum



Befeuert durch

- Angriffsattraktivität
 - Gesundheitsdienstleister verfügen über eine riesige Menge an persönlichen Informationen, die für Betrug verwendet werden können
- Fachkräftemangel
 - 40'000 fehlende Cyber-Spezialisten in der Schweiz (Quelle NZZ, Nov. 2019)
 - 3.5 Mio offene Jobs weltweit
 - Nahezu 0% Arbeitslosenquote von Cyber Spezialisten seit 2011
- Arbeitnehmermarkt
 - Wahl des Arbeitgebers
 - Extrinstische vs. Intrinstische Motivation



Warum dieser Anstieg?

- Leicht verfügbare Technologien für Cyberkriminelle (Baukasten im Darknet)
- Stark ansteigende Nutzerzahlen im Internet
- Grosser Anreiz für Kriminelle (aus Schwellenländern mit niedrigem Einkommen)
- Neue "Zentren" für Cyberkriminalität (z.B. Brasilien, Indien, Nordkorea und Vietnam)
- Kryptowährungen ermöglichen das Cashing ohne Spuren zu hinterlassen



Opfer und Entwicklung

- Im Fokus steht jede Organisation, die Geld hat.
- Fälle von Cybercrime im Gesundheitswesen werden sich vervierfachen!
- Bis 2021 wird weltweit alle 11 Sekunden ein Unternehmen einem Lösegeld-Angriff zum Opfer fallen
- Ransomware ist die am schnellsten wachsende Form der Cyberkriminalität.



Es ist nicht die Frage ob...

Finanzielle Folgen 20.08.2019, 19:15 Uhr

Cyberangriff kostet Meier Tobler Millionen

Weil Hacker die gesamte IT-Infrastruktur der Haustechnikerfirma Meier Tobler lahmlegten, konnte das Unternehmen während vier Arbeitstagen keine Waren ausliefern. Nun ist klar: Der Schaden geht in die Millionenhöhe.



MEISTGELESENE

Neon: die Schweizer Internet-Bank im Test

27.06.2019



Die 10 besten Notiz-Apps für das iPad mit Pencil-Support

08.01.2019



Das neue iPhone SE im



Managed Security Service



1. Vorstellung Galexis
2. Anfängliche Herausforderungen
3. UMB Managed Security Service
 - OnBoarding
 - Schwachstellen Management
 - Endpoint Detection and Response
 - Security Monitoring (SIEM)
 - Security Architektur
4. Laufende Weiterentwicklungen der Security Services



Vorstellung Galexis

- Galexis ist ein Unternehmen der Galenica Gruppe und gehört deren Geschäftsbereich Services an
- Galexis ist der führende Vollgrossist und Dienstleister im Schweizer Gesundheitsmarkt und gleichzeitig das Bindeglied für alle beteiligten Akteure
- Das umfassende Produkte- und Dienstleistungsangebot beliefert über 7'200 Kunden: Apotheken, Ärzte, Drogerien, Heime und Spitäler
- ~ 800 engagierte Mitarbeiter arbeiten in den beiden Distributionszentren
- Täglich > 445'000 Packungen werden versendet



Vorstellung UMB AG





400

**Kolleginnen
und Kollegen**

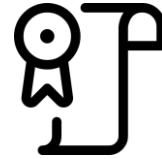


100%

**Inhabergeführt
und unabhängig**



**Nr. 1
Dun &
Bradstreet**



**weit über 1'000
Technologie
Zertifizierungen**



Seit 2012. Beste Arbeitgeberin der Schweiz

Great
Place
To
Work®

Best Workplaces™

Switzerland

GREAT
PLACE
TO
WORK

Best
Companies
to Work for 2012
Switzerland



GREAT
PLACE
TO
WORK

Best
Companies
to Work for 2014
Switzerland



GREAT
PLACE
TO
WORK

Best
Companies
to Work for 2016
Switzerland



GREAT
PLACE
TO
WORK

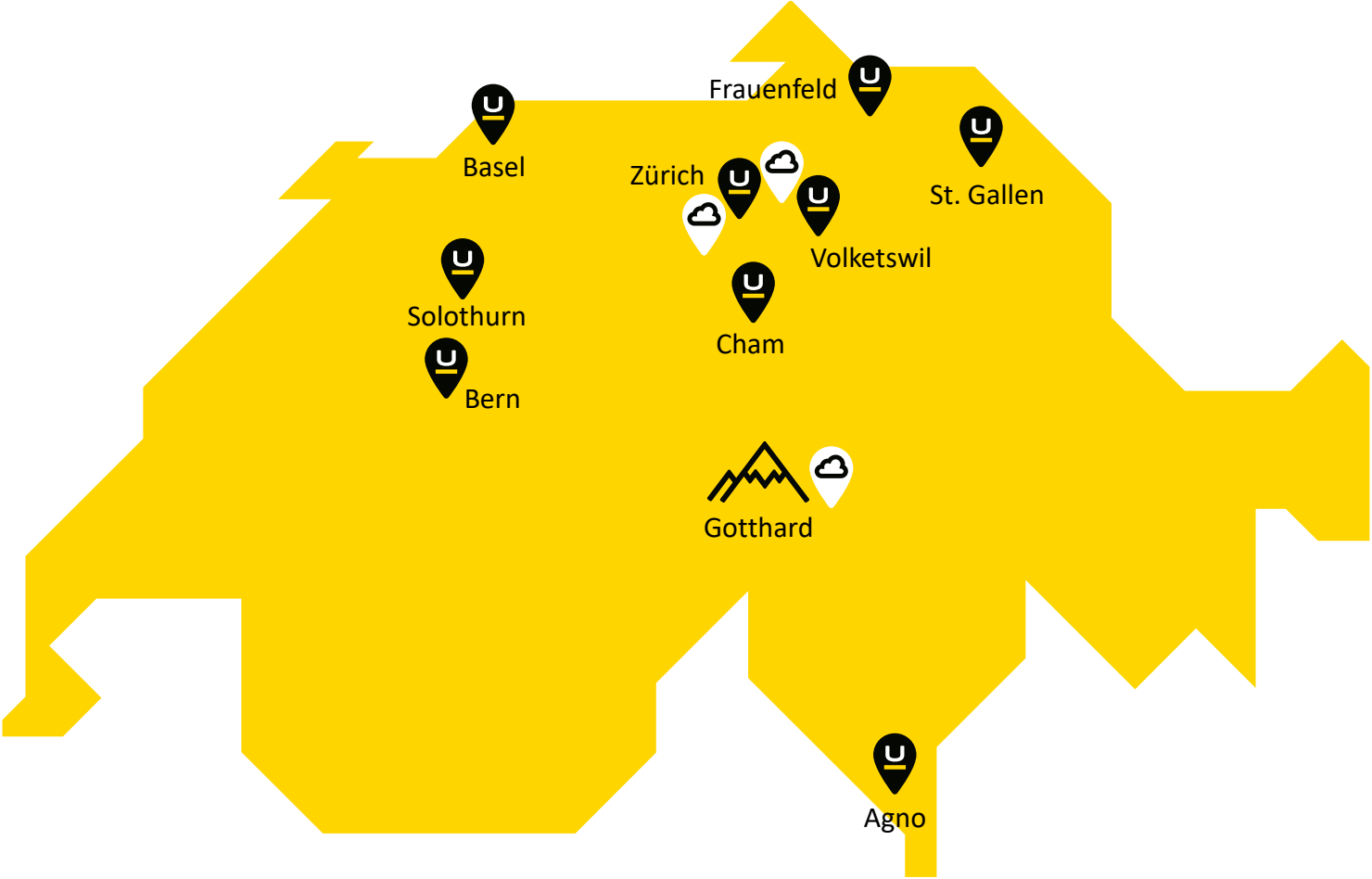
Best
Companies
to Work for 2018
Schweiz



Best
Large
Workplaces™

Great
Place
To
Work.

SCHWEIZ
2020



Frauenfeld

Basel

Zürich

St. Gallen

Solothurn

Volketswil

Bern

Cham

Gotthard

Agno

Business



Consulting



Sourcing



Collaboration



Digitalisierung



Digital Workplace



Transformation

Technology



Cloud



Linux & Container



SAP



Plattform



Security



Strategische Partner



Plattform

Compute & Storage

- Compute & Storage
- File & Object Storage
- Cloud Storage Tiering

Virtualisierung

- Hypervisor
- vGPU Workload Management

Data Management

- Backup & Recovery
- Langzeitaufbewahrung
- Disk to Disk / Tape

Connectivity (Network & Protection)

- Software Defined Networking (SDN)
- Software Defined WAN (SDWAN)
- Zero Touch Deployment
- LAN
- WLAN
- Firewall

Database

- SQL
- Oracle
- HANA

Mainframe

- Z System
- LinuxOne
- Secure Service Container für App & Blockchain
- Pervasive Encryption (Encryption at Rest)
- GDPR / PCI
- MongoDB & Postgres



Cloud

Cloud Services

- IT as a Service
- Infrastructure as a Service
- Platform as a Service
- Workplace as a Service
- Device as a Service
- Digitalization as a Service
- Network as a Service
- Security as a Service
- Disaster Recovery as a Service
- Backup as a Service

- SAP as a Service
- Storage as a Service
- IBM Power as a Service
- Container Platform as a Service

MultiCloud

- Cloud Management Portal
- Hybrid Cloud
- Cloud Governance
- Cloud Security

Public Cloud

- Microsoft Azure
- AWS
- SAP
- Oracle

Cloud Connectivity

- Cloud Connect
- Express Route



Security

Security Services

- Cyber & Cloud Security
- Vulnerability Management
- Security Risk Assessment
- Perimeter Security
- Risk Management & Compliance
- Notfallkonzept
- Security Awareness
- Penetration Test
- Forensic
- Security Information & Event Management (SIEM)
- Security Awareness



Sourcing

Services

- Cloud Services
- Managed Services
- DueDiligence & IT Assessment
- Betriebskonzept Design
- Incident & Problem Management
- Change Management
- Event Management
- Capacity & Availability Management
- Release & Deployment Management
- Continuity Management

- Service Level Management

- Automation
- Reporting

Support

- ServiceDesk
- 24/7 Pikett & Monitoring

Fazit:

Cyber Security sollte ganzheitlich betrachtet werden. Ein umfassender Schutz wird durch die Kombination aus Security Awareness, Technologien und Spezialisten erreicht.

Danke für Ihre Zeit



UMB

creating time®