xtention
IT with care.

Gesundheitsdaten im Visier:

Darknet-Bedrohungen erkennen, verstehen und abwehren

Ing. Peter Brillinger, MSc
Team Lead Cybersecurity Competence Center

Vorstellung

xtention

Ing. Peter Brillinger, MSc

- Teamleiter Cybersecurity Competence Center
- Seit 2021 bei x-tention Informationstechnologie in Wels

Ausbildung

- Sichere Informationssysteme – FH Hagenberg
  Bachelor und Master
- HTBLA Wels - Informationstechnologie

Zertifizierungen

- ISMS-Manager und -Auditor nach ISO 27001:2013 (TÜV Austria)
- Certified Project Management Associate IPMA (pma)
- Verschiedene produktbezogene Zertifizierungen

Vom IT-Startup zur internationalen Unternehmensgruppe

xtention

Über 1.000 Kunden weltweit, mehr als 800 Mitarbeiter und mehr als 20 Jahre Erfahrung

xtention IT with care.

xD it for industries

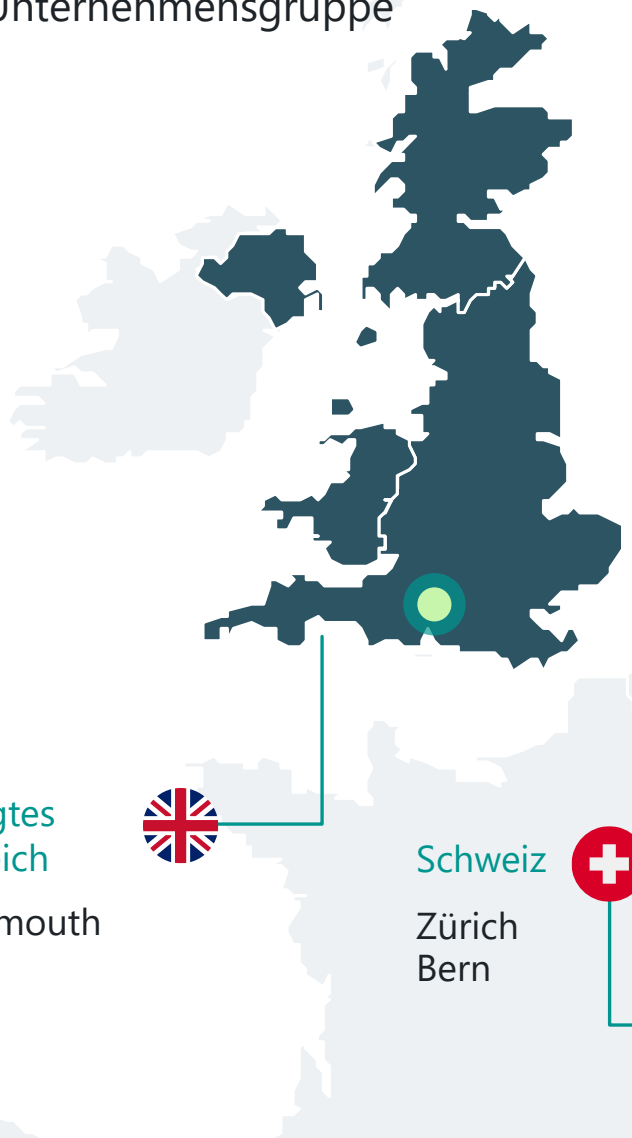
xtention IT with care.

solvistas

2001	2011	2012	2018	2019	2023
Gründungsjahr	Markteintritt Schweiz	Markteintritt Deutschland	Gründung Faktor D und Übernahme it for industries	Markteintritt UK	Übernahme von solvistas
Betrieb, IT-Dienstleistungen im Gesundheitswesen					
		Softwarelösungen für das Gesundheitswesen			
			Beratung zu Digitalisierung und Transformation		
			ERP-Lösungen für mittelständische Unternehmen in der Industrie		
					Data Science und Software Solutions

Unsere 14 Standorte weltweit

x-tention Unternehmensgruppe



Vereinigtes Königreich

Bournemouth

Schweiz

Zürich
Bern

Deutschland

Heidelberg
Berlin
Augsburg
Oberhausen

Österreich

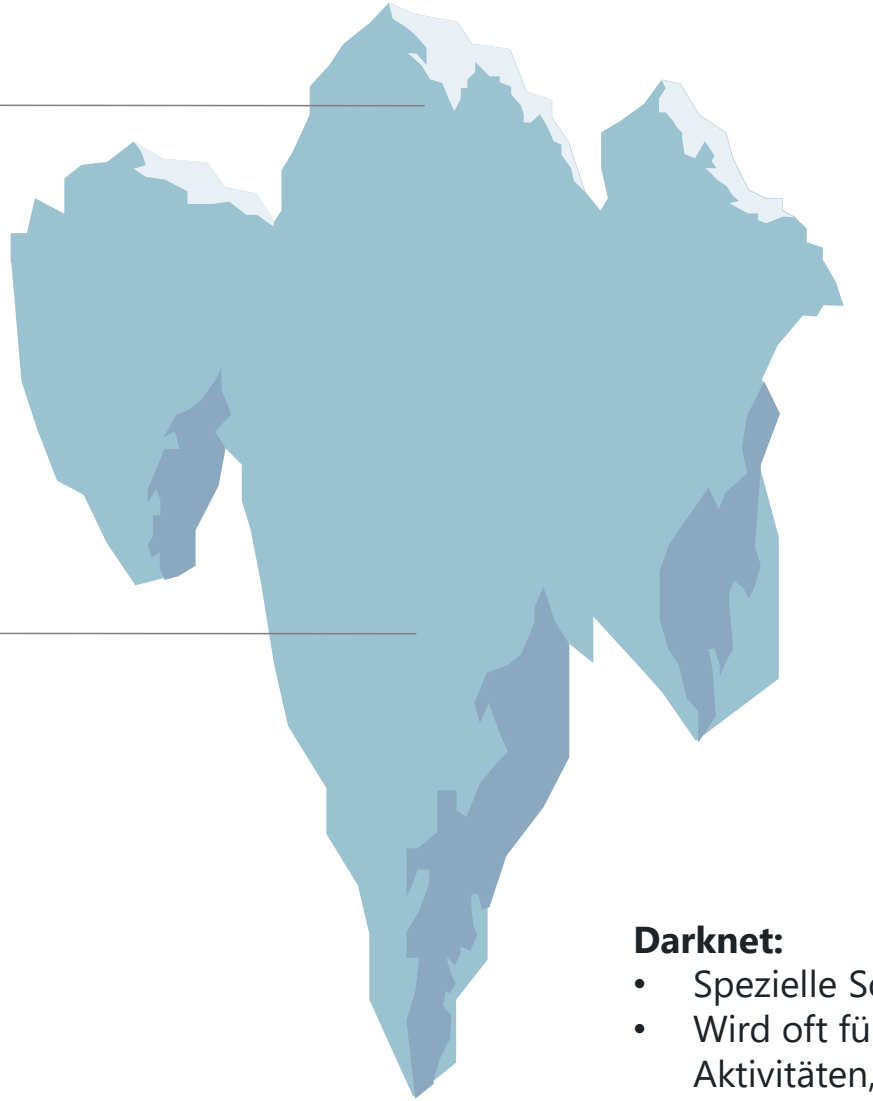
Wels
Wien
St. Peter / Au
Graz
Salzburg
Klagenfurt
Linz

Wieviel Prozent des Internets sind Teil des Clear Webs?

xtention

Clear Web **~5%**

- Auch “Surface Web”
- Öffentlich zugängliche Webseiten, via Suchmaschinen zugreifbar
- Beispiel: x-tention.com



Deep Web & Darknet **~95%**

Deep Web:

- Nicht indexiert oder indexierbar
- Beispiele:
  - Private Datenbank
  - Wissenschaftliches Archiv
  - Medizinische Aufzeichnungen

Darknet:

- Spezielle Software erforderlich (Tor, I2P)
- Wird oft für anonyme Kommunikation und Aktivitäten, die nicht verfolgt werden sollen verwendet
- Schwer abgrenzbar/durchsuchbar

xtention
IT with care.

xtention

Relevanz für den Healthcare-Sektor?

xtention

Beispiele aus dem Darknet

xtention

Schlüssel zum Erfolg: **Prävention und Reaktion**

Empfehlungen

Empfehlungen

xtention

- **Vorbereitung auf einen Incident**
  - Incident Playbooks und Notfallhandbücher
  - Es gibt keine 100% akkurate Vorbereitung, jedoch ~70%
  - Auf Erfahrung von Dienstleistern setzen
- **Schwachstellen-Monitoring**
  - Intern / Extern
  - Vulnerability Scans und Attack Surface Management
  - In Kombination mit Patchmanagement
- **Multifaktor-Authentifizierung**
  - Zweiter Faktor = zusätzliche Hürde für Angreifer
- **DNS Traffic Monitoring (und Blocking)**
  - Auch IoT-Geräte und Gebäudeleittechnik beachten
  - Sehr wirksam gegen Phishing-Angriffe und als zusätzliche Schutz-Ebene zur bestehenden Firewall

Empfehlungen

xtention

- **Zentrale Protokollierung**
  - Entfernte Aufbewahrung relevanter Logs
  - Je länger, desto besser (Minimum: 90 Tage)
- **Keine Administrationsrechte auf lokalen Geräten**
  - Bei Notwendigkeit nur temporäre Ausnahmen (z.B. LAPS)
- **Angriffserkennung der nächsten Generation**
  - EDR / NDR / XDR
  - Nächste Generation ist wichtig, um fortgeschrittene Angreifer erkennen
  - Auf Dienstleister mit entsprechender Erfahrung und Kenntnissen setzen (Beachtung von HealthCare-Spezifika)
- **Passwort-Manager**
  - Unterschiedliche und starke Passwörter

Empfehlungen

xtention

- **Abgesicherte Backup-Infrastruktur**
  - Offline-Backups vorhalten
  - Online-Backup-Infrastruktur wirksam absichern (z.B. WORM), gehärtete Linux-Systeme
- **Netzwerksegmentierung**
  - Unterteilung des Netzwerks in kleinere, separate Subnetze, um Auswirkungen von möglichen Angriffen zu reduzieren
- **Kontinuierliche Darknet-Überwachung**
  - Alarmierung bei Findings
  - Sofortige Aktion bei neuen Leaks / Keyloggern oder Datensätzen, um schlimmeres zu verhindern
  - Ziel: Schneller sein als Angreifer

360° Sicherheit durch x-tention Cybersecurity Services

xtention

xtention
IT with care.

Vielen Dank für Ihr Interesse & Ihre Aufmerksamkeit

Ing. Peter Brillinger, MSc
Cybersecurity Competence Center

E-Mail Peter.Brillinger@x-tention.at
Telefon +43 7242 2155 6100

x-tention Informationstechnologie GmbH
Römerstraße 80A, 4600 Wels, Österreich
Margot-Becke-Ring 37, 69124 Heidelberg, Deutschland

x-tention.com