IT-Sicherheit aktuell

Gefahren, Risiken und mögliche Gegenmaßnahmen

23.06.2022

Florian Meigel

- 20+ Jahre Erfahrung in der IT
- in einem Mittelstandskonzern in der Filmbranche
- fast 10 Jahre verantwortliche Position Informationssicherheit
- 4 Jahre verantwortliche Position Datenschutz
- 2014 Gründung IT works

ALLES AUS EINER HAND
- ein Ansprechpartner für alle IT-nahen Themen

KEEP IT SIMPLE
- hohe Stabilität
- niedrige Kosten
- effiziente Prozesse

IT works

- externe IT-Abteilung
- schnelle Reaktionszeiten
- kostengünstig durch Standardisierung
- kompetente, persönliche Ansprechpartner
- proaktive Überwachung Ihrer IT-Landschaft

VOLLUMFASSENDE IT-BETREUUNG

- vom Helpdesk bis zur sicheren Standortvernetzung

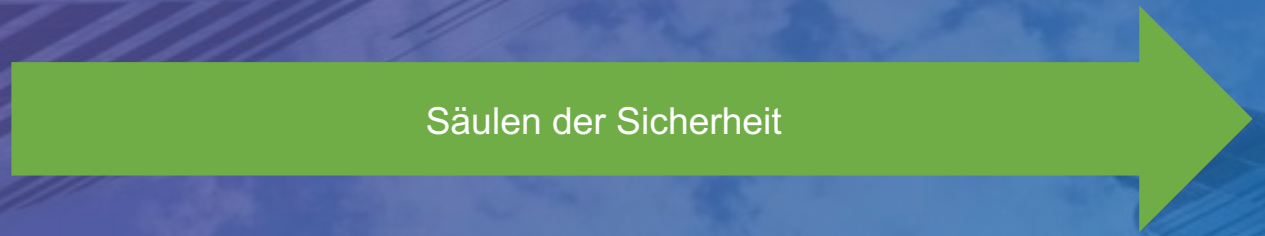
INFORMATIONSSICHERHEIT

- Security Audits
- Begleitung externer Audits & Zertifizierungen
- eigene E-Learning Plattform für Ihre Mitarbeiter

DATENSCHUTZ

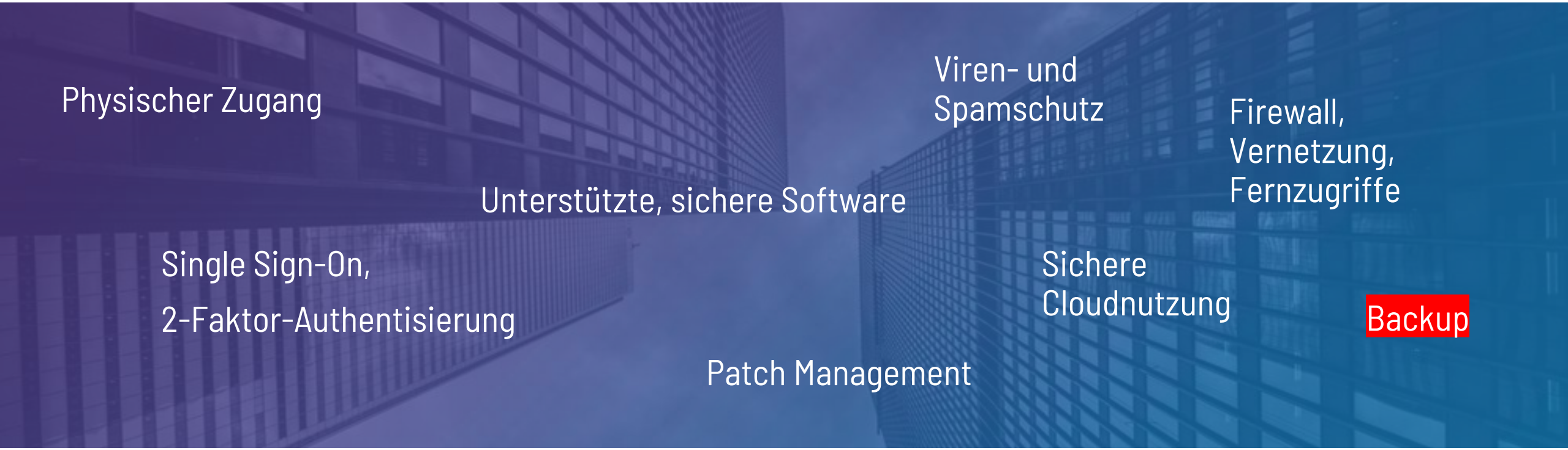
- pragmatische Ansätze
- eigenes Fachpersonal

100% Sicherheit gibt es nicht.



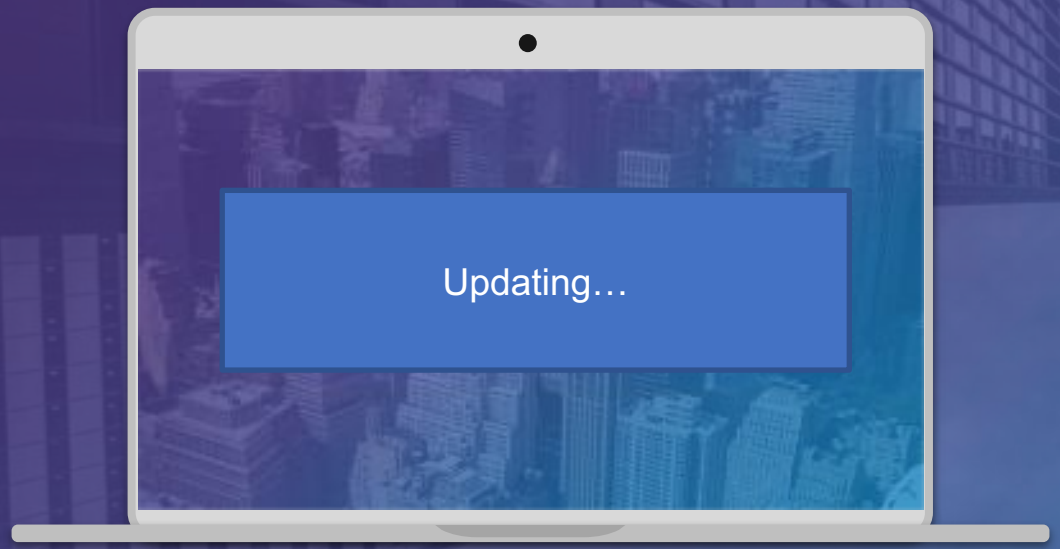
Technik Prozesse Mensch

Faktor Technik



Aktuelle Standards sind heute leicht und schnell zu implementieren.

Virenscanner



Ein Virenscanner arbeitet meist basierend auf Signaturen.

Er kann nur erkennen, was ihm über Signaturen vorher „beigebracht“ wurde.

Zwischen Schadsoftware-Programmieren und Virenscanner-Herstellern herrscht ein regelrechtes Katz-und-Maus-Spiel.

Virenscanner sind wichtig und ein effizientes Mittel. Jedoch ist Mitdenken gefordert!

Verschlüsselungstrojaner / Ransomware 1

Einmal geladen, durchläuft Ransomware die Netzlaufwerke und verschlüsselt alle Dateien mit Schreibrecht.

Eine Entschlüsselung durch IT ist nicht möglich.

Der Schlüssel kann teuer gekauft werden – falls man ihn erhält.

Verschlüsselungstrojaner / Ransomware 2

Aktuelle Fälle

Landmaschinenhersteller Fendt/AGCO:
05.05.-17.05. keine Produktion möglich

Landesregierung Kärnten:
Arbeitsunfähig, viele Daten veröffentlicht
24.05.-?
Lösegeld: 5 Millionen

Medizinische Universität Innsbruck:
Kein Datenzugriff, Datensätze nach und nach im Internet.
21.06.-?

Gegenmaßnahmen

- mehrere Virenscanner-Instanzen
- aktuelle Sicherheitsupdates
- Mitarbeiter-Trainings: Alle. Regelmäßig. Aktuell.
- Incident Response Plan
  sofort Experten mit Vorkenntnissen hinzuziehen!
- Backups

Sicherheitsupdates / Patches

- ausschließlich aktuelle Betriebssysteme betreiben!

- kritische Updates für Systeme und Applikationen zeitnah einspielen!
  wir empfehlen vorab Tests an unkritischen Systemen.

- Verpflichtung zur Mitwirkung aller Mitarbeiter

- IT-Abteilung benötigt Wissen über kritische Updates für die eingesetzte Software

Aktuelle kritische Sicherheitslücke: “Follina”

Vor Kurzem wurde eine kritische Lücke bekannt, über die Angreifer allein durch die Vorschau von Microsoft-Dokumenten beliebigen entfernten Code ausführen konnten.

Mit den Windows Updates vom 14.06. wird diese Lücke geschlossen.

Weisen Sie Ihre IT-Abteilung an, alle Windows-Systeme zeitnah zu aktualisieren!

Sicherungen / Backup

- kritische Daten identifizieren
  z.B. Microsoft 365 Cloud?

- Vorhaltezeiten definieren!
  wie lange dauert es bis ich einen Schaden bemerke?

- Backups Offsite & Offline ablegen!
  nicht zugreifbar für z.B. Verschlüsselungstrojaner

- Monitoring
  laufen meine Backups zuverlässig?

- Revocery Tests
  regelmäßige Wiederherstellungs-Übungen kritischer Daten und Server

Faktor Prozesse

Prozesse sollten sich der vorhandenen Technik anpassen, um effizient zu sein.

Security Policy: Wichtige Bestandteile

Password Policy

Sichere Passwörter, Umgang mit Passwörten

2-Faktor-Authentisierung

Access Policy

Welche Geräte dürfen ins Netz? Gästenetz für alles andere!

Need to Know Prinzip

Privatnutzung

Cloud Policy

Welche Dienste sind sicher?

Standards setzen

Admin-Rechte

Separate Konten

Nur für IT und Entwickler.

Dauerhaftes Arbeiten mit erhöhten Rechten birgt Risiken!

Faktor Mensch

Einhalten der Policies

Teilnahme an Trainings

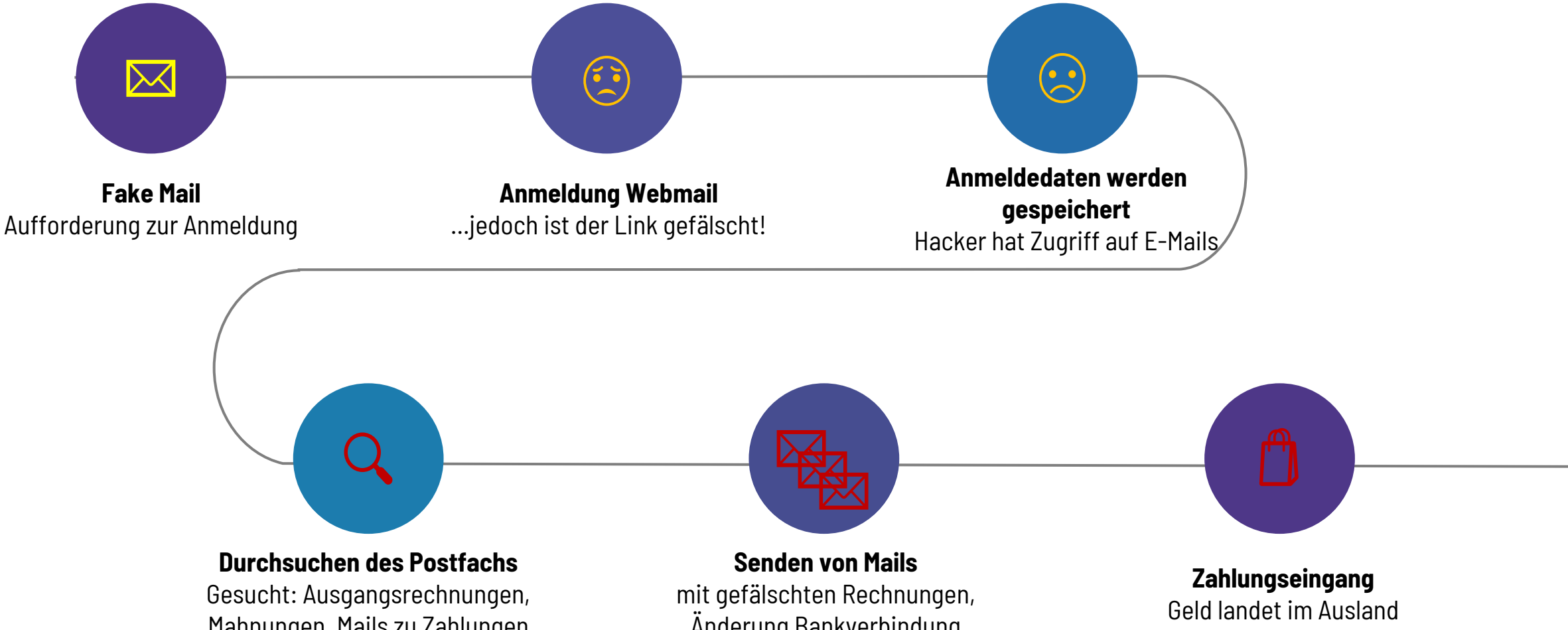
Vorfälle erkennen und melden

vermeintlicher Komfort-Verzicht

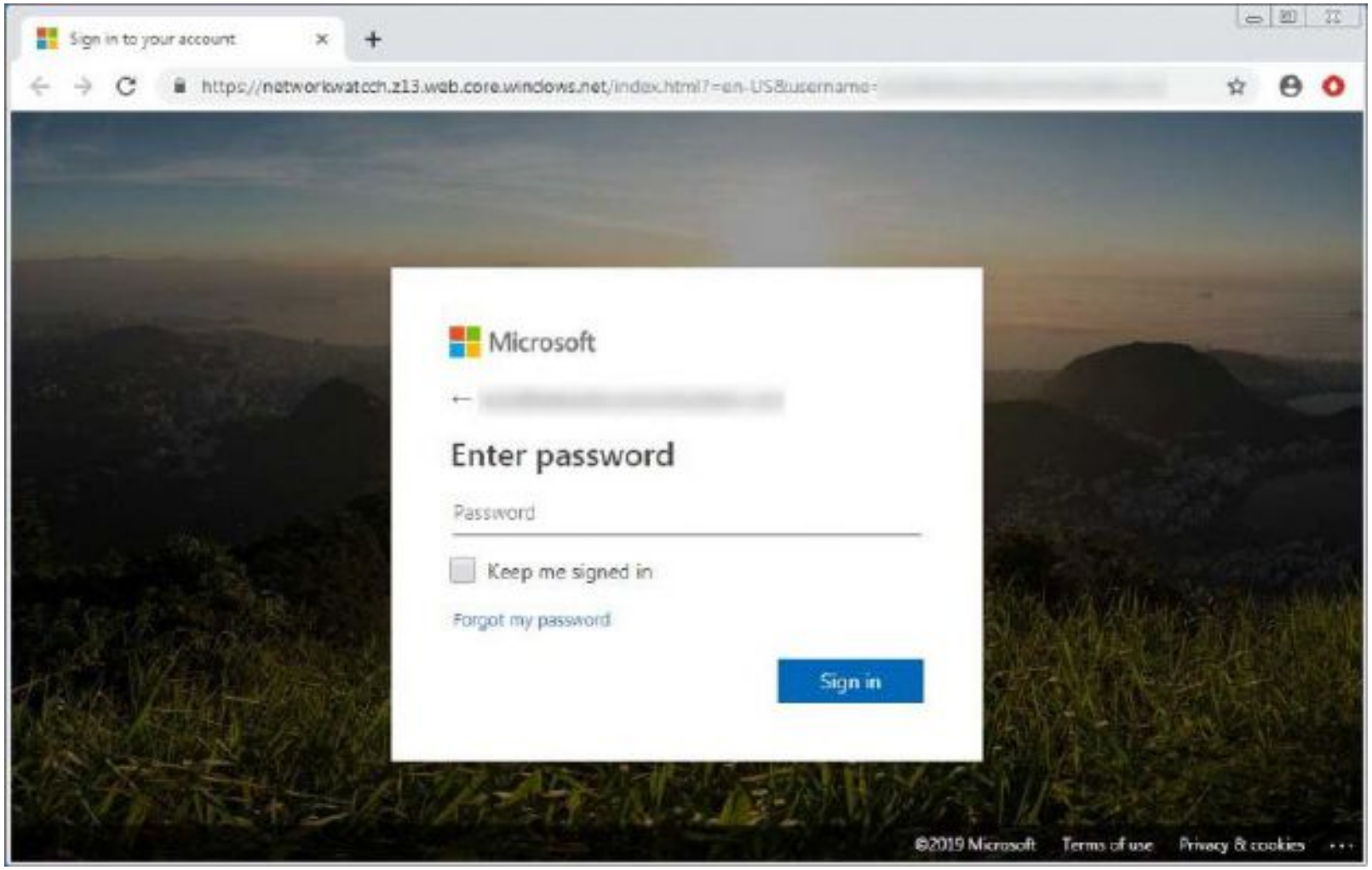
Awareness

Der Mensch ist am leichtesten anzugreifen!

Phishing- Angriff: Rechnungsbetrug



Fake Microsoft Portal

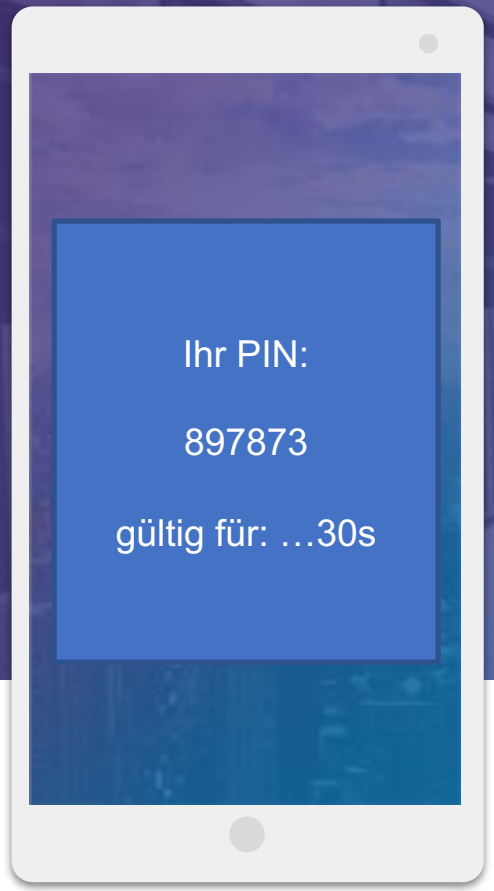


Kenne ich die Funktion?

Auf Infomails/Warnungen achten!

Microsoft Portal: Logo?

Gegenmittel 2-Faktor-Authentisierung



2-Faktor-Authentisierung ist ein einfaches Gegenmittel!
Selbst mit dem Passwort kann sich ein Hacker nicht mit Ihren Daten anmelden.

Einfach und kostengünstig einzuführen für:

Microsoft365 (E-Mail!),

viele Web-Portale oder Cloud-Anbieter

Auch für Fernzugriffe (z.B. VPN) sollte heute 2-Faktor-Authentisierung verwendet werden! Oft kommt durch Single Sign-On dasselbe Passwort zum Einsatz!

weitere Phishing-Angriffe

- CEO-Fraud
- falscher Microsoft-Mitarbeiter
- falscher IT-Mitarbeiter

Es gibt viele bekannte, sehr erfolgreiche Methoden über Social Engineering Geld zu verlieren.

Sorgen Sie durch Schulung Ihrer Mitarbeiter vor!

Audits

Lassen Sie sich von externen Profis autitieren.
Nicht erst wenn es zu spät ist!

Sicher haben Sie eine gute IT-Abteilung –
doch 4 Augen sehen mehr.

Sorgen Sie mit geplanter Unterstützung für den Notfall vor.

Datenschutz

Erfolgreiche Hacks sind oft auch Datenschutz-Pannen!

Verletzung der Meldepflicht von 72 Stunden:

Gemäß Art. 83 Nr. 4 DSGVO sind Bußgelder bis zu 20 Millionen Euro oder bis zu 4 Prozent des weltweiten Vorjahresumsatzes möglich.

Thank You

Zeit für Fragen!

Florian Meigel

Tel: 08039 497 00 00

E-Mail: info@it-works.biz

www.it-works.biz