Netree

Cyber Security
im Zeichen der digitalen Transformation

Daniel Bühlmann – Partner / CTO

V 1.00 / November 2021

Der Perimeter hat sich verändert...

Netree

Modern Perimeter

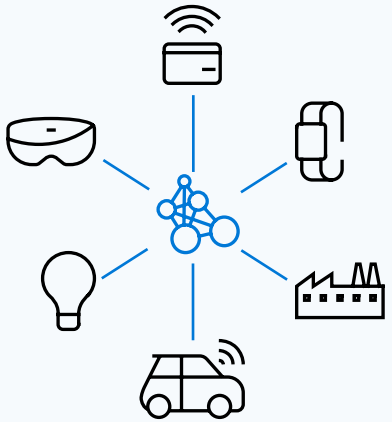
Cloud Technologien

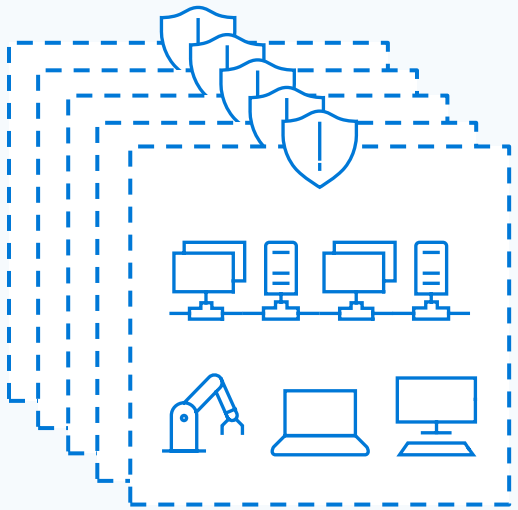
Software as a Service (SaaS)

Platform as a Service (PaaS)

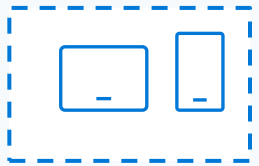
Infrastructure as a Service (IaaS)

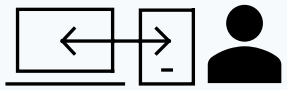
Internet of Things (IoT)





On-Premises Infrastrukturen





Mobilität und Flexibilität

Die Gefahr ist real und kann jeden treffen...

Netree

LÖSEGELD

Nach Cyber-Angriff: Erpresser erhöhen Druck auf Peter Spuhlers Stadler Rail

Die Cyberkriminellen, die Anfang Mai ins IT-Netzwerk des Schienenfahrzeugbauers Stadler eingedrungen sind, haben mutmasslich einen zweiten Teil der gestohlenen Daten im Darknet veröffentlicht. Sie wollen ein Lösegeld erpressen, beissen aber auf Granit.

Schweizer Industriekonzern von Cyberattacke lahmgelegt

Der Milliardenkonzern Omya fährt schrittweise Werke in 50 Ländern wieder hoch. Ein Sprecher erklärt, was los ist.

Omya, ein international tätiger Schweizer Hersteller von Industriemineralien, war letztes Wochenende aufgrund eines Cyberangriffs gezwungen, den Betrieb in allen Werken einzustellen.

Trojaner-Befall: Emotet bei Heise

Jürgen Schmidt 06.06.2019

Cybercrime, Emotet, Emotet-bei-heise, Malware, Ransomware, Trojaner, Windows, Windows 10

Es gab einen schwerwiegenden Einbruch in das Heise-Netz; Auslöser war eine Emotet-Infektion. An der Beseitigung arbeiten aktuell die IT-Abteilungen der Heise Gruppe und weitere Spezialisten.

Kurzvorstellung

Netree

Daniel Bühlmann

«Perfektion ist nicht dann erreicht, wenn es nichts mehr hinzuzufügen gibt, sondern wenn man nichts mehr weglassen kann»

Antoine de Saint-Exupéry

Firma: **Netree AG** | 4658 Däniken | 35 MitarbeiterInnen

***Expertise**: Cloud/Hybrid, Modern Workplace & Security*

***Unsere Kunden**: Regionale KMUs & CH Education*

Job: Mitgründer & CTO

Email: daniel.buehlmann@netree.ch

1. Backup, Backup, Backup…
2. Intelligenter E-Mail Schutz
3. Built-in Security Features aktivieren

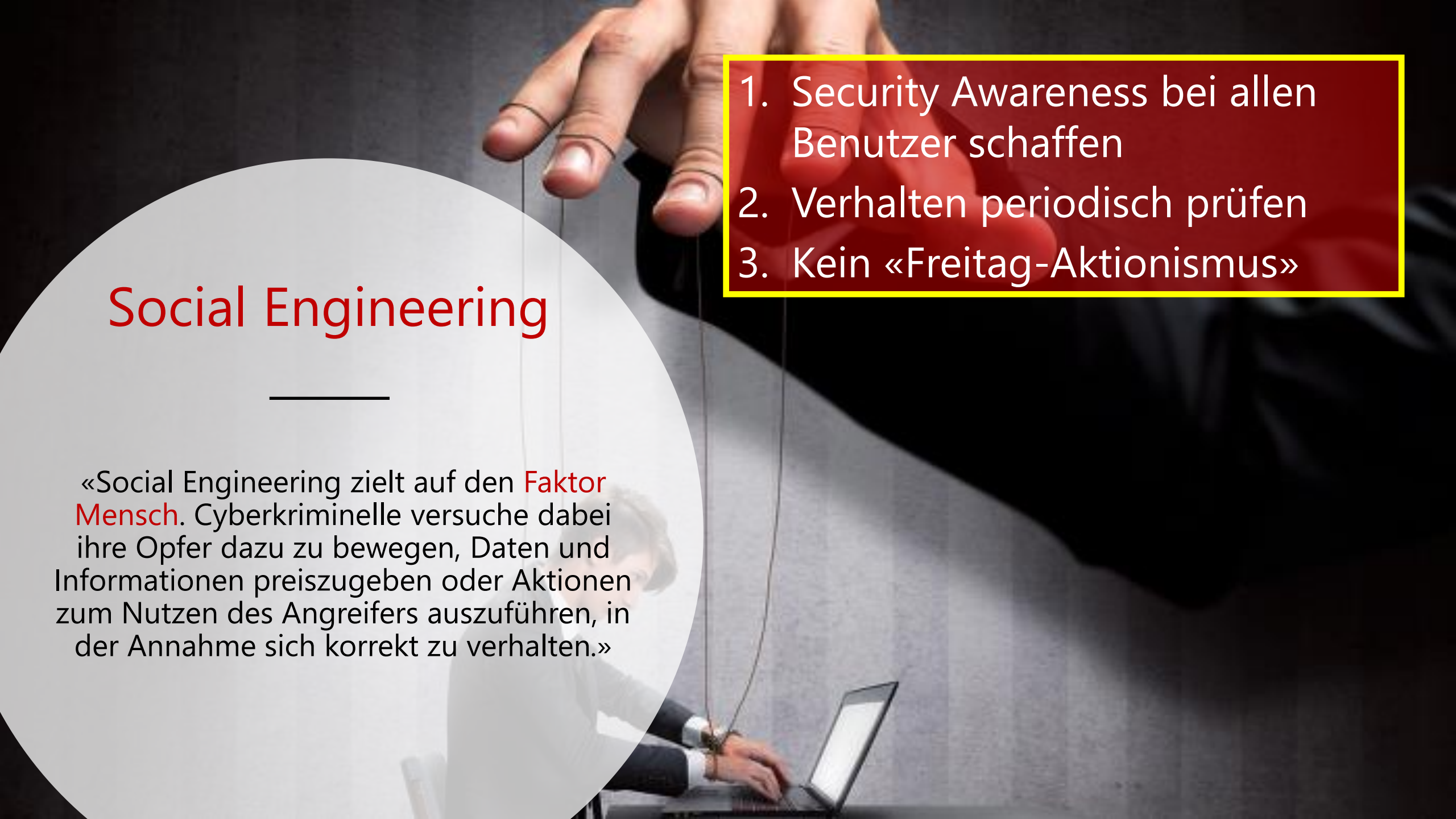
Ransomware

«Als Ransomware bezeichnet man spezielle Schadsoftware, die mittels eines Verschlüsselungstrojaner Nutz- und/oder Systemdaten automatisch verschlüsselt. Für die Entschlüsselung oder nicht-Veröffentlichung werden im Anschluss Lösegelder (engl. «ransom») eingefordert.»

1. Minimale Rechte bei allen Arbeiten
2. Multi Faktor Authentifizierung (MFA)
3. Conditional Access

Phising / Identity

«Unter dem Begriff Phishing (Neologismus von fishing, engl. für "Angeln") versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit z.B. Identitätsdiebstahl zu begehen.»



1. Security Awareness bei allen Benutzer schaffen
2. Verhalten periodisch prüfen
3. Kein «Freitag-Aktionismus»

Social Engineering

«Social Engineering zielt auf den Faktor Mensch. Cyberkriminelle versuche dabei ihre Opfer dazu zu bewegen, Daten und Informationen preiszugeben oder Aktionen zum Nutzen des Angreifers auszuführen, in der Annahme sich korrekt zu verhalten.»

Advanced Persistens Threats

«Bei APT Attacken handelt es sich um Cyber-Angriffe die es gezielt auf einzelne Unternehmen abgesehen haben. Die Angreifer versuchen dabei unerkannt eine dauerhafte «Präsenz» im internen Netzwerk des Unternehmens zu erlangen. Zumeist mit dem Ziel relevanten Daten und Informationen unbemerkt über längere Zeiträume zu entwenden.»

1. Update, Update, Update…
2. Extended Detection & Response Lösungen
3. Security Operation Center

Das sollten wir nicht vergessen…

Netree

…soweit wir wissen, gibt es uns bekannte Erkenntnisse. Es gibt also Dinge, die wir kennen und die wir wissen.
Wir wissen auch, dass es bekannte Unbekannte gibt. Das heisst, wir wissen, dass es einige Dinge gibt, die wir nicht wissen.
Aber es gibt auch uns nicht bekannte Unbekannte, von denen wir nicht wissen, dass wir sie nicht kennen.

Donald Rumsfeld, 12.2.2002, Department of Defense news briefing

Vielen Dank für ihre Aufmerksamkeit

www.netree.ch