KRALOS

Carsten Klein | CEO & Founder, KraLos GmbH

„Die entscheidende Frage ist nicht, ob Ihr Unternehmen angegriffen wird – sondern was passiert, wenn es passiert.“

DIE UNBEQUEME FRAGE

Wie sicher ist Ihr Unternehmen wirklich?

KRALOS

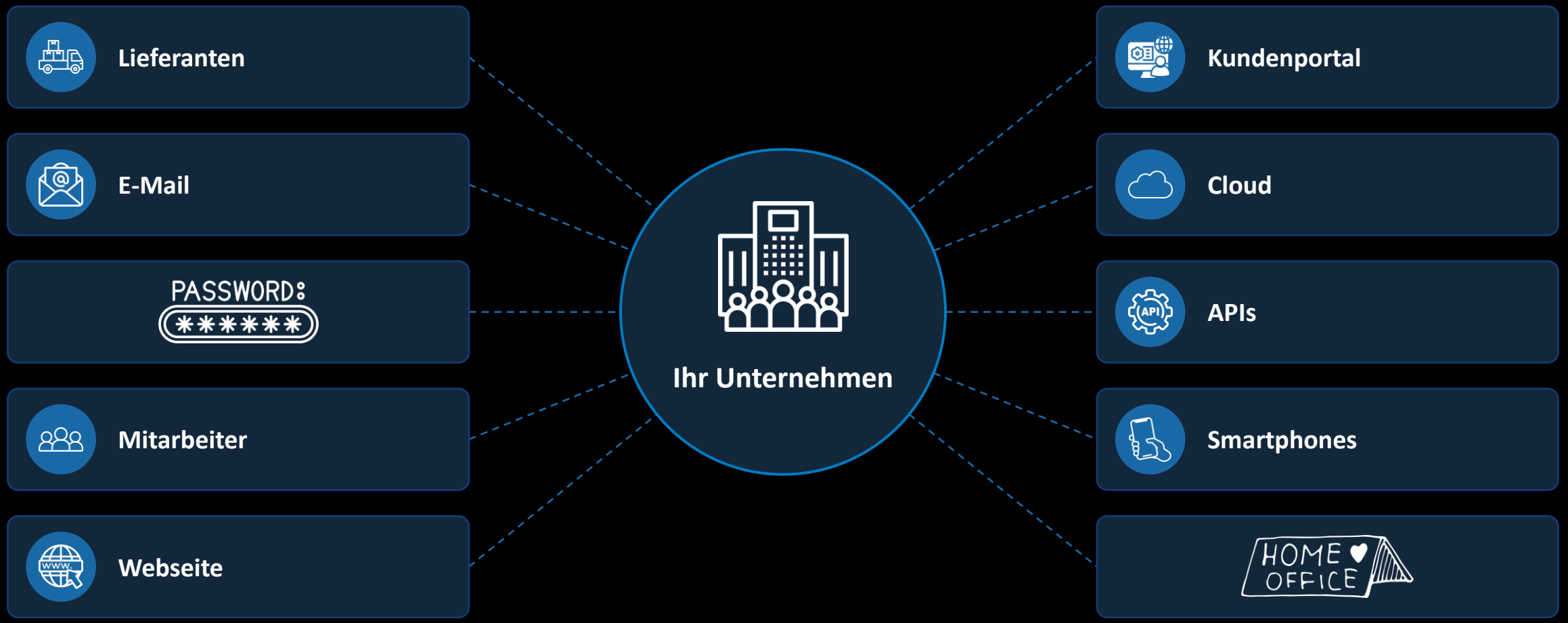
?	?	?	?	?
Firewall?	**Virenschutz?**	**MFA?**	**Backups?**	**Security-Tools?**

Viele Unternehmen können genau aufzählen, welche Sicherheitslösungen sie einsetzen.

Deutlich schwieriger wird die Antwort auf die Frage, was bei einem echten Angriff tatsächlich passiert.

Ihre Angriffsfläche ist größer als Sie denken

KRALOS



Ein Angriff beginnt oft unspektakulär

Cyberangriffe sind häufig keine einzelnen Ereignisse. Sie sind Ketten von kleinen Erfolgen.

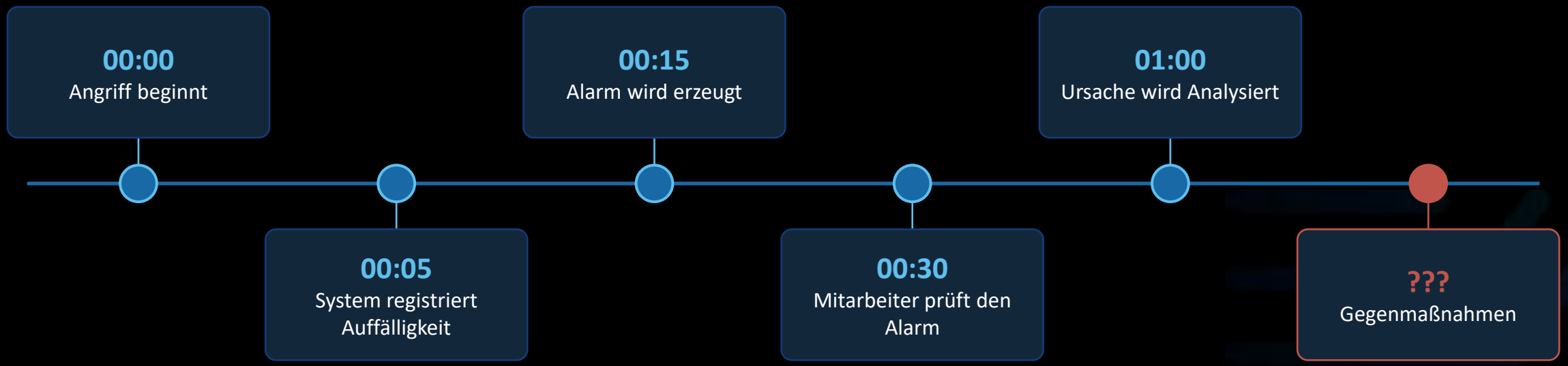
Eine E-Mail ▶ **Ein Klick** ▶ **Eine gefälschte Anmeldung** ▶ **Ein gestohlener Zugang** ▶ **Zugriff auf ein System**

Unbekannte Schwachstelle ▶ **Webanwendung** ▶ **internes System** ▶ **Daten**

Ein Unternehmensproblem

Das eigentliche Problem: Zeit

Was passiert zwischen Angriff und Reaktion?



Und was macht der Angreifer in dieser Zeit?

Mehr Security ≠ automatisch mehr Sicherheit

Wie viele Security-Produkte brauchen Sie eigentlich?

- WAF
- SIEM
- MFA
- SOC
- IDS
- DDoS
- Anti-Bot
- FIREWALL
- Monitoring
- E-Mail-Security
- Backup

Jedes neue System erzeugt auch neue Komplexität.

Mehr Systeme ▶ mehr Schnittstellen ▶ mehr Konfiguration ▶ mehr Meldungen ▶ mehr Aufwand

Die Qualität Ihrer Cybersecurity misst sich nicht an der Anzahl Ihrer Tools.

Was gute Cyber Security wirklich ausmacht

Gute Cyber Security beginnt mit Architektur.

1. **REDUZIEREN**
   Angriffsfläche verkleinern
2. **AUTOMATISIEREN**
   nicht auf jede Reaktion eines Menschen warten
3. **TRENNEN**
   kritische Systeme isolieren
4. **WEITERFUNKTIONIEREN**
   auch unter Angriff handlungsfähig bleiben
5. **VALIDIEREN**
   Zugriffe nicht einfach vertrauen
6. **SCHÜTZEN**
   Daten und Kommunikation absichern

Secure by Design statt Security by Addition.

STRATEGIE

Der 60-Sekunden-Sicherheitscheck

Können Sie diese 6 Fragen beantworten?

1. Welche Systeme Ihres Unternehmens sind aus dem Internet erreichbar?
2. Was passiert, wenn morgen eine unbekannte Schwachstelle ausgenutzt wird?
3. Wie schnell erkennen Sie einen Angriff?
4. Was passiert automatisch – und wo muss ein Mensch reagieren?
5. Sind Ihre sensiblen Informationen auch geschützt, wenn ein System kompromittiert wird?
6. Können Sie sicher sagen, wer oder was auf Ihre Systeme zugreifen darf?

✓ **Dann kennen Sie Ihre Sicherheitsarchitektur sehr gut.**

→ **Dann wissen Sie zumindest, wo Sie anfangen sollten.**

Cyber Security neu denken

Von reaktiv zu präventiv

Klassischer Ansatz

- ANGRIFF
- ERKENNEN
- ALARMIEREN
- ANALYSIEREN
- REAGIEREN

Moderner Ansatz

- ANGRIFFSFLÄCHE REDUZIEREN
- SYSTEME TRENNEN
- ZUGRIFF VALIDIEREN
- ANGRIFFE ABWEHREN
- AUTOMATISIERT REAGIEREN

Das Ziel sollte nicht sein, einen Angriff möglichst schnell zu bemerken.

Das Ziel sollte sein, dass er möglichst wenig erreichen kann.

KRALOS

CYBER SECURITY NEU GEDACHT.

Digital Trust Intelligence Platform

WEBOUNCER

Webouncer

Schutz für alle Web Anwendungen –
verhindert Angriffe.

SHADOWKEY

Shadowkey

Sicherer Datentransfer.
Verschlüsselt, bevor die Daten Ihr Gerät verlassen.

PHISHING-GUARD

Phishing-Guard

Multichannel Protection

Verstehen. Begrenzen. Schützen.

Fragen?