SCHUTZSCHILD FÜR IHR UNTERNEHMEN

Sicherheit und Datenschutz

T · · Systems ·

SICHERHEIT UND DATENSCHUTZ: VIELE HANDLUNGSFELDER

SO SCHÜTZEN SIE IHRE SENSIBLEN DATEN UND SYSTEME

Datenschutz

- Kundendaten schützen
- Anonymisierung bei Analytics-Anwendungen
- Sichere digitale Identität

Datensicherheit

- Sichere Kommunikation
- Sichere Datenhaltung
- Schutz von Unternehmens-geheimnissen

Ausfallsicherheit

- Erreichbarkeit von Online-Shops
- Redundante Systeme (z. B. Filialanbindung)
- Sicherstellung von Zahlungsmöglichkeiten

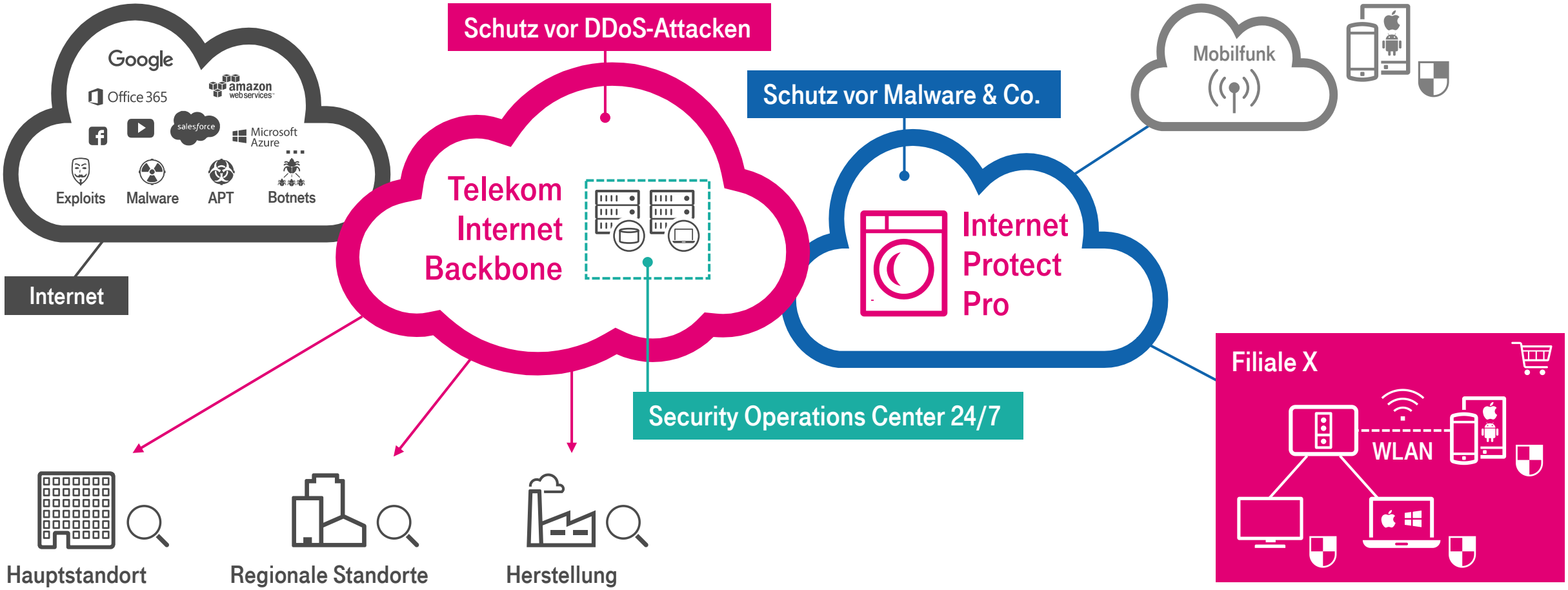
Schutz vor Angriffen

- Schutz vor Malware
- Incident-Reporting und -Management
- Gefahrenwarnsysteme

T · · Systems ·

T-SYSTEMS SECURITY SERVICES: KOMPLETTES SCHUTZSCHILD

FÜR HANDELSUNTERNEHMEN AN ALLES GEDACHT



DDOS PROTECTION: 3 VARIANTEN, EINZIGARTIGER SCHUTZ

DAS MODULARE PAKET GEGEN BOTNETZ-ANGRIFFE

Unser Partner: ARBOR NETWORKS

Mit einem DDoS-Angriff (Distributed Denial of Service) **überlastet ein Angreifer Ressourcen** seines Opfers, so dass **z. B. Webshops für Käufer nicht mehr erreichbar sind.**

Die Folgen

Unzufriedene Kunden, Produktionsausfall, finanzielle Verluste, Rufschädigung

Die Lösung

DDoS Protection

Schützt vor allen Formen von DDoS-Angriffen, **unabhängig von Komplexität, Stärke und Dauer der Attacken.**

- Schutz des Netzwerkzugangs als auch der Systeme und Applikationen
- Modulares und skalierbares Lösungskonzept
- Sowohl Cloud- als auch dedizierte Lösungen
- Niedrige Anfangs-Investitionskosten
- Niedrige Betriebskosten durch Standardisierung und Automatisierung
- Sofort verfügbare DDoS Protection

Cloud Web DDoS-Schutz	**On Premise** DDoS-Schutz	**Backbone** DDoS-Schutz
Schutz gegen komplexe und Volumenattacken	Schutz gegen komplexe Attacken	Schutz gegen Volumen-attacken
Aus der Cloud für lokale und gehostete Systeme	Am Kundenstand-ort für die lokale Infrastruktur	Im Telekom Backbone für den Internet-Access
Für Web-Services	Für Systeme & Applikationen	Für den Internet-Access & Bandbreite

INTERNET PROTECT PRO: EINFACH SICHERER

ATTACKEN BEREITS IN DER CLOUD ERKENNEN & ISOLIEREN

Unser Partner: zscaler

Seit 2015 müssen Unternehmen laut IT-Sicherheitsgesetz definierte Sicherheitsstandards umsetzen. Bisherige Schutzmaßnahmen reichen nicht, um die **Flut an Bedrohungen wie Cyberattacken, Datenlecks und immer neuer Schad-Software zu bewältigen.**

Die Folgen

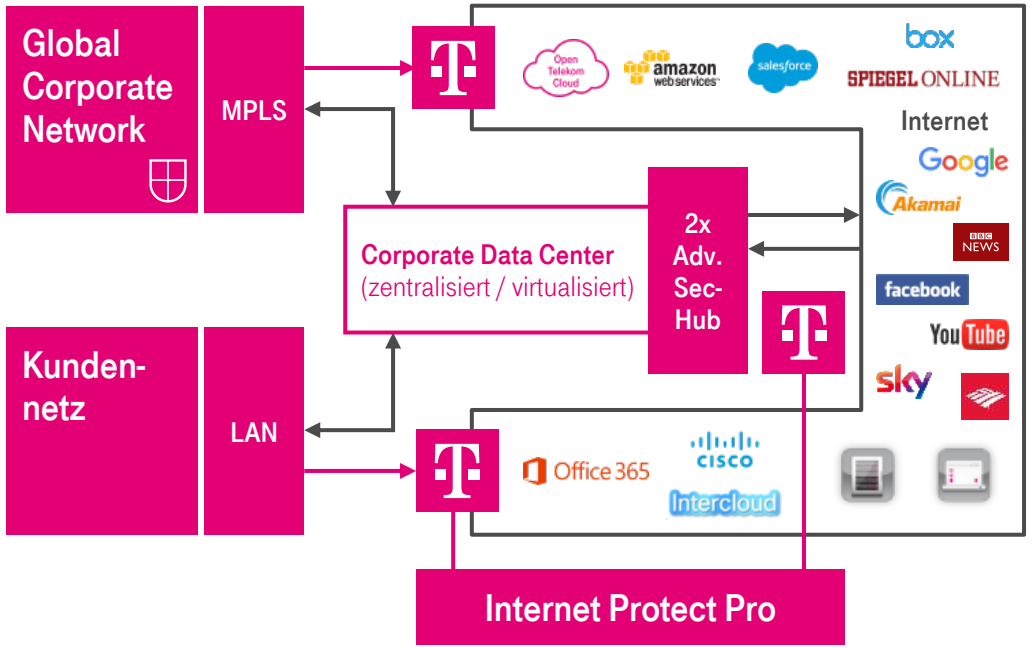
Einnahmenverlust, niedrigere Produktivität, Verlust von Geschäftsgeheimnissen

Die Lösung

Internet Protect Pro

Das Cyberschutzschild in der Cloud kann Schadcode, Cyberangriffe, Datendiebstahl in Echtzeit blockieren – **einfach zu konfigurieren und einzusetzen.**

- Funktionen eines Advanced Security Hubs aus der Telekom Cloud
- Schutz vor bekannten und unbekanntem Schadcode
- Kein Invest beim Kunden erforderlich
- Alle Kundendaten nur in den hochsicheren Rechenzentren der Telekom



CYBER DEFENSE FÜR DEN MITTELSTAND: INTELLIGENT!

SAMMLUNG UND ANALYSE VON LOG UND NETZWERKDATEN

Basiert auf USM:

Industriespione wollen Know-how abgreifen und nehmen **geschäftskritische Prozess-abläufe ins Visier.** Hierfür wird Schad-Software genutzt, von der es täglich hunderttausende neue Varianten gibt.

Die Folgen

Wettbewerbsvorteil wird verspielt, Reputation geht verloren, Entschädigungs-zahlungen, unzufriedene Kunden

Die Lösung

Cyber Defense für den Mittelstand

Mehr Sicherheit und Über-blick durch die zentrale, unkomplizierte Lösung mit Echtzeit-Überwachung, die **mehrstufige Angriffe zuverlässig abwehrt.**

- Schnelle, kostengünstige Out-of-the-Box-Security-Lösung zur Erfassung des Ist-Zustands und aktuelle Gefahrenabwehr für die bestehende IT-Umgebung
- Zentrale Bereitstellung und Betrieb in sicheren Telekom Rechenzentren oder beim Kunden vor Ort
- Sensoren in der Umgebung der Kundensysteme sammeln die notwendigen Daten und senden diese an die Telekom
- Um das Bereitstellen der Hardware, die Lizenzen, Überwachungen, Wartung sowie Störungen kümmert sich die Telekom
- Speziell ausgebildete Experten der Telekom übernehmen das Überwachen und Auswerten von Sicherheitsvorfällen – in Echtzeit

Ein Lagebild in Echtzeit ermöglicht die **Erkennung unberechtigter Zugriffe** und die **frühzeitige Reaktion.**

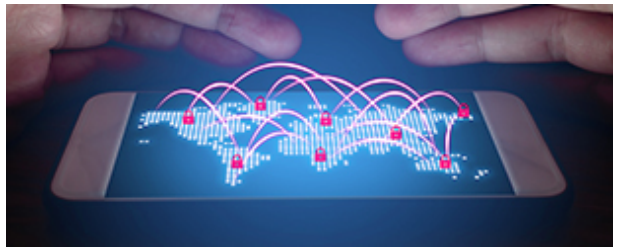
USM = Unified Security Management

MOBILE PROTECT PRO: SICHERHEIT IN DER TASCHE

DIE NEUE DIMENSION MOBILER SICHERHEIT

Powered by: ZIMPERIUM

Mobile Endgeräte rücken zunehmend in den Fokus von Cyberkriminellen, da **die Geräte von Mitarbeitern oft nicht ausreichend gesichert sind.** Dabei genügt ein infiziertes Gerät, um dem Unternehmen nachhaltig zu schaden.



Die Folgen

Erpressbarkeit durch Datenklau, Verlust von Firmengeheimnissen, finanzielle Einbußen

Die Lösung

Mobile Protect Pro

Schützt Unternehmen und ihre Mitarbeiter in Echtzeit **gegen das gesamte Spektrum von Angriffen auf Endgeräte, Netze und Anwendungen.**

Geräteschutz

Netzwerkschutz

Applikationsschutz

Parameterüberwachung

Anomalieerkennung

zConsole: Reporting, Policies, Forensik

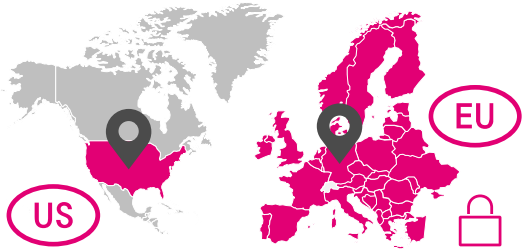
Mobile Protect Pro bietet in einer Lösung Sicherheit für mobile Applikationen, Schutz gegen Attacken über drahtlose Verbindungen und gegen Schwachstellen in mobilen Betriebssystemen – **Risikobewertung und Gefahrenabwehr in einem.**

DATENSCHUTZ MADE IN GERMANY
FEST VERANKERT IN UNSERER PRODUKT-DNA

Anwendungen	Collaboration	Infrastruktur	Arbeitsplatz
SAP, salesforce	Microsoft, UNIFY	HUAWEI, CISCO	Microsoft, CITRIX

Wie werden Daten durch T-Systems verarbeitet?

Angemessenes Datenschutzniveau wird durch Binding Corporate Rules of Privacy (BCRP) oder EU-Standard-vertragsklauseln weltweit sichergestellt.



Alle Lösungen werden nach deutschem Datenschutz betrieben!

Privacy & Security Assessment

- Integriertes Verfahren für technische Sicherheit und **Datenschutz als Bestandteil der Produkt- und Systementwicklungsprozesse**
- Gewährleistet ein **einheitliches und adäquates Sicherheits- und Datenschutzniveau** in allen Produkten, Systemen und Plattformen, die aktualisiert oder neu erstellt werden

Beachtung der deutschen und EU-Datenschutzbestimmungen!

- Die Leistungen werden von T-Systems selbst oder durch Dienstleister im Wesentlichen aus Standorten in D oder im EU-Rechtsraum erbracht
- Daten in deutschen Rechenzentren von T-Systems unterliegen den deutschen bzw. europäischen Datenschutzbestimmungen und werden durch die Datenschutzbehörden extern kontrolliert
- Erforderliche Übermittlungen in außereuropäisches Ausland i.d.R. auf Basis von Binding Corporate Rules oder EU-Standvertragsklauseln

T · · Systems ·