KFK IT von Mensch zu Mensch.

# Das neue EU-Datenschutzrecht

## Ein Überblick und Umsetzungstipps für die IT

Referent: Sascha Brugger

KFK Büro- und Kommunikations Technik GmbH

DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND

# Aktuelle Technologien (Cyber Security)

- Geänderte weltweite Sicherheitslage
- Wie die Hacker arbeiten
- Verpflichtungen aus der europäischen DSGVO
- Was kann ich dagegen tun? - Was mache ich wenn etwas passiert ist?
- Wie behalte ich die Kosten im Griff?
- Lösungsmodelle im Überblick
- VDS 3473 / 10010

# Veränderte weltweite Sicherheitslage

Die veränderte weltweite Sicherheitslage zwingt uns zum Handeln und zum Überdenken der aktuellen Sicherheitsansätze.

Bislang waren Hacker eher in kleineren Gruppen organisiert und haben sich bewusst Ziele ausgesucht (Verbreitung politischer Meinungen, Industriespionage).

Heute ändert sich das Bild dahingehend, dass vermehrt ungezielt auf die breite Masse angegriffen wird. Sinn ist hier die Verbreitung von Erpressungstrojanern. Die Daten der Opfer werden verschlüsselt und somit unbrauchbar gemacht. Erst durch Zahlung eines Lösegeldes werden die Daten (hoffentlich) wieder entschlüsselt. Diese Angriffe werden nicht mehr von kleinen Gruppen sondern von Staaten organisiert (Nordkorea).

# Veränderte weltweite Sicherheitslage

Es sei hier ausdrücklich erwähnt, dass nicht die Verschlüsselung durch Erpressertrojaner das Problem darstellt (ausgelagerte Backups), sondern der ungehinderte und unbemerkte Abfluss der Daten. Durch den Abfluss von Daten zu Kriminellen wird eine noch höhere Erpressbarkeit geschaffen.

# Veränderte weltweite Sicherheitslage

Staaten greifen großflächig andere Staaten oder Länder an. Sie versuchen so an Geld zu kommen um ihre Waffenentwicklung zu finanzieren (Beispiel: WannaCry Nordkorea).

**Fazit:**
Oftmals sind die üblichen Sicherheitsstrukturen diesen Bedrohungen nicht mehr ausreichend gewachsen.

Daraus ergeben sich speziell für Unternehmen, die mit besonders schützenswerten Daten arbeiten, erhöhte Anforderungen.

# Verpflichtungen aus der DSGVO

**Neue Grundsätze DSGVO**
Rechtmäßigkeit, Treu und Glauben, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht.

**Bereits bekannte Grundsätze aus dem BDSG die angepasst wurden**
Transparenz, Zweckbindung, Datenminimierung (Datensparsamkeit)

**Schlagwöter aus der DSGVO**
Ausreichend, regelmäßig, Stand der Technik, innovativ

# Neue Lösungsansätze. Ganzheitliche IT

Wir brauchen Lösungen, die den ganzheitlichen Ansatz verfolgen. Einzelne Sicherheitskomponenten reichen NICHT aus. Ein ganzheitlicher Ansatz setzt sich aus folgenden Komponenten zusammen:

**Effektiver Schutz vor Ransomware (Verschlüsselungtrojaner)**
Proaktive Erkennung aller PC im Netzwerk. Sobald ein Verschlüsselungstrojaner zu arbeiten beginnt, muss dieses Gerät vom Netz, um eine Ausbreitung zu verhindern.

**Datensicherung vom Netzwerk geografisch trennen**
Die Datensicherung sollte in die Cloud ausgelagert werden. So ist sichergestellt, dass es immer eine Sicherung aller Daten gibt, falls das lokale Netzwerk kompromittiert wurde. Zusätzlich können hier Kosten durch Sicherungsbänder und Sicherungshardware eingespart werden.

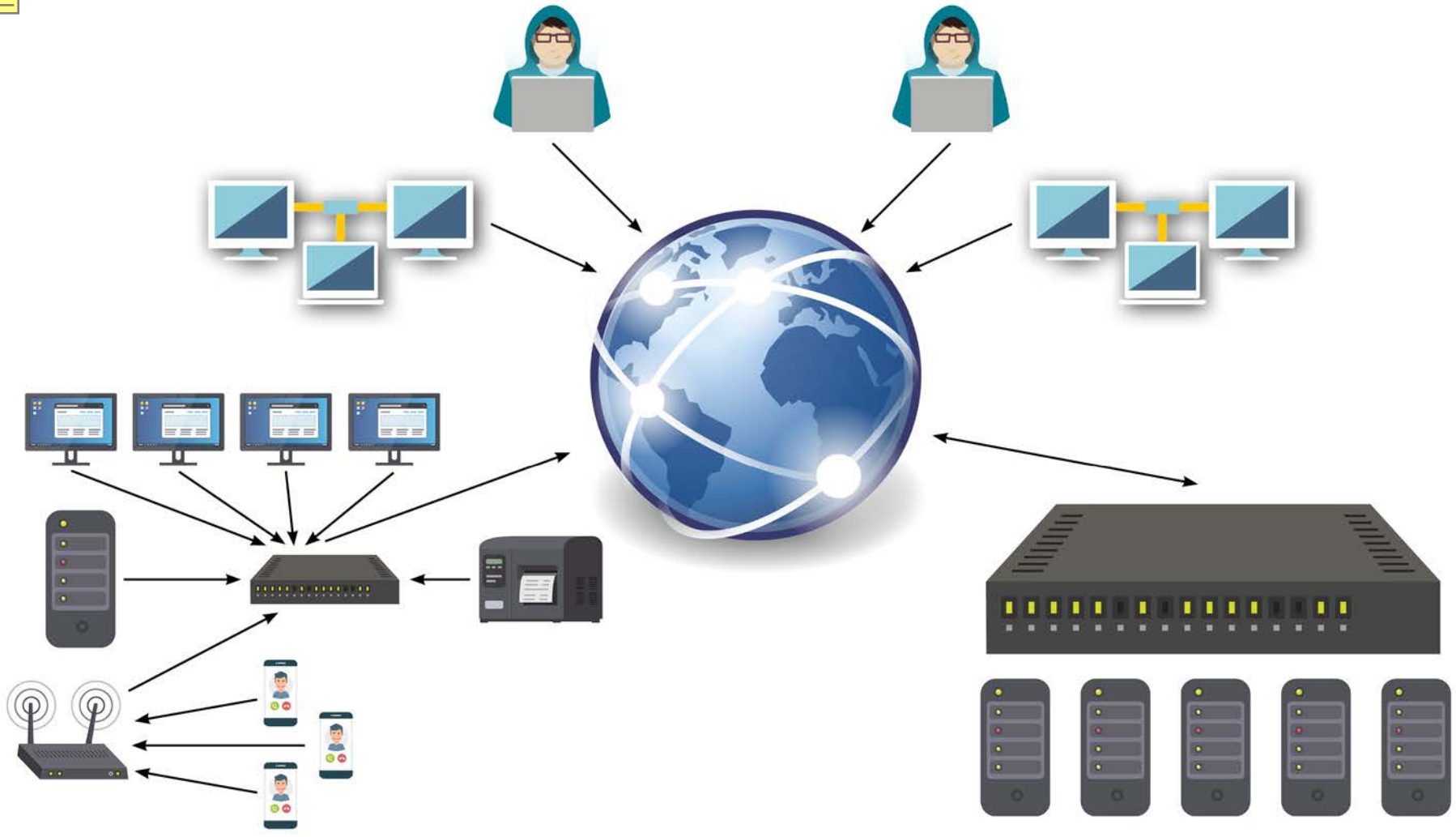
# Neue Lösungsansätze. Ganzheitliche IT

## Effektiver Mailschutz

Die meiste Schadsoftware kommt nach wie vor als Trojaner, der an einer E-Mail angehängt ist, ins Netzwerk. Innovative Software nach modernen Richtlinien kann hier einen effektiven Schutz bieten. Cloud-basierte Systeme bieten hier die Möglichkeit sehr viel schneller zu reagieren, wenn irgendwo weltweit eine Infektion ausbricht. Netzwerke können schon geschützt werden, noch bevor die Infektionswelle das eigene Netzwerk erreicht. Wenn man davon ausgeht, dass ca. 6% aller empfangenen Mails einen Hacking-Hintergrund haben, können mit diesen Maßnahmen eine Senkung in den 0,XXX% Bereich realisiert werden.

## Managed Firewall

Hackerangriffe haben oftmals deshalb Erfolg, weil im allgemeinen Tagesgeschäft wichtige Routineaufgaben vernachlässigt oder vergessen werden. Oftmals kommen Infos über z.B. neue Firmwareupdates nicht beim Admin an.



# Neue Lösungsansätze. Ganzheitliche IT

Bei einer gemanagten Firewall übernehmen diese Aufgabe die Spezialisten des Betreuers (Systemhaus). Hier sorgen die internen Prozesse dafür, dass ein optimierter Schutz gewährleistet ist (Mitarbeitergruppen, die nur diese Aufgaben haben). Zusätzlich muss hier von Kundenseite kein Knowhow aufgebaut werden. Hohe Investitionen für Hardware, Carepacks und Softwarepflegeverträge fallen weg (vom Dienstleister zeigen lassen ▶ ADV).

## Komplettüberwachung aller Geräte im Netzwerk

Das Monitoring oder die gezielte Überwachung von Hardware bezieht sich heute meist auf Server. Die Client-Arbeitsstationen werden hier gerne übersehen und nicht ausreichend überwacht. Das stellt ein besonders hohes Risiko dar, denn die meisten Angriffe finden am Arbeitsplatz und nicht am Server statt. Deshalb ist es besonders wichtig, dass hier ein optimaler Schutz gewährleistet ist (aktuelle Updates, Patches, Signaturen, etc.).

# Kosten im Griff behalten

Die Auslagerung und Ausweitung sicherheitsrelevanter Dienste muss nicht unbedingt mit einem starken Anstieg der damit verbundenen Kosten einhergehen. Es ergeben sich dadurch auch Potentiale, an anderer Stelle Kosten einsparen zu können.

Einsparpotentiale durch Auslagerung:

- Hardwarekosten werden reduziert
  - Firewall-Hardware
  - Sicherungshardware wie Server, Sicherungsbänder und Bandgeräte
  - Mailserver Hardware
- Stromkosten (ca. 50€ pro Server/Monat inkl. Klimaanlage)
- Lizenzkosten können reduziert werden: Durch den Kauf großer Lizenzpakete, die unter vielen Kunden aufgeteilt werden, können Kosten reduziert werden.

# Kosten im Griff behalten

Die ständige Weiterbildung der Mitarbeiter im Security-Bereich wird teilweise auf den Dienstleister verschoben.

Die Administratoren des Kunden werden teilweise von den Routinearbeiten entlastet und können sich um die tagesaktuellen Themen kümmern. Dadurch werden Überlastungssituationen entschärft und die Arbeiten in der Firma können schneller erledigt werden (Fehlervermeidung).


06
Schulung
01
Managed Firewall
05
Backup
360°
Hosting
02
Mail Appliance
04
Monitoring
03
Managed Endpoint
Security

# Fazit / Zusammenfassung

Vorteile der ganzheitlichen IT Sicherheitsbetrachtung (360 Grad):

- Kunde braucht sich um das komplette Thema IT-Sicherheit nicht mehr zu kümmern (Beschaffung der Hardware, Weiterbildung der Mitarbeiter, große Erstinvestitionen, Patchmanagement, Updates, etc.)
- Sehr schnelle Reaktionszeiten im Falle eines Angriffs: Oftmals schon vor dem Eintreffen der Angriffswelle
- Planbare IT: Planbare Kosten pro Monat pro Gerät.
- Alle benötigten Wartungskosten im Vertrag inkludiert
- Starke Reduzierung des organisatorischen Aufwands
- Einhaltung rechtlicher Forderungen (Europäische DSGVO / Mailarchivierung / etc.)

# Informieren Sie Ihre Mitarbeiter

# Welche Fragen sind noch offen?

Sie haben Fragen zu Ihrer IT oder benötigen Hilfe bei der Implementierung oder Umstellung? Sprechen Sie uns gerne an! Wir sind für Sie da!

**Sascha Brugger**
Consultant

Tel.: +49 681 98844 51
Fax.: +49 681 98844 22
E-Mail: sascha.brugger@kfk-gmbh.de
**www.kfk-gmbh.de**

**Patrick Franz**
Marketingmanager

Tel.: +49 681 98844 18
Fax.: +49 681 98844 22
E-Mail: patrick.franz@kfk-gmbh.de
**www.kfk-gmbh.de**

KFK IT von Mensch zu Mensch.

# Vielen Dank für Ihre Aufmerksamkeit!

KFK Büro- und Kommunikations Technik GmbH

DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND