

„Ist E-Mail-Verkehr heute noch sicher?“

Olaf Otahal
solutionIT GmbH



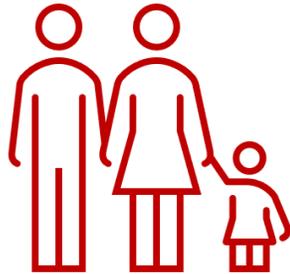


Aktuelle Bedrohungslage



#ITklugesichert

Gesellschaft



Identitätsdiebstahl

Erpressung

Fake-Shops im Internet

Wirtschaft



Ransomware

Schwachstellen, offene oder falsch konfigurierte Online-Server

IT-Supply-Chain: Abhängigkeiten und Sicherheit

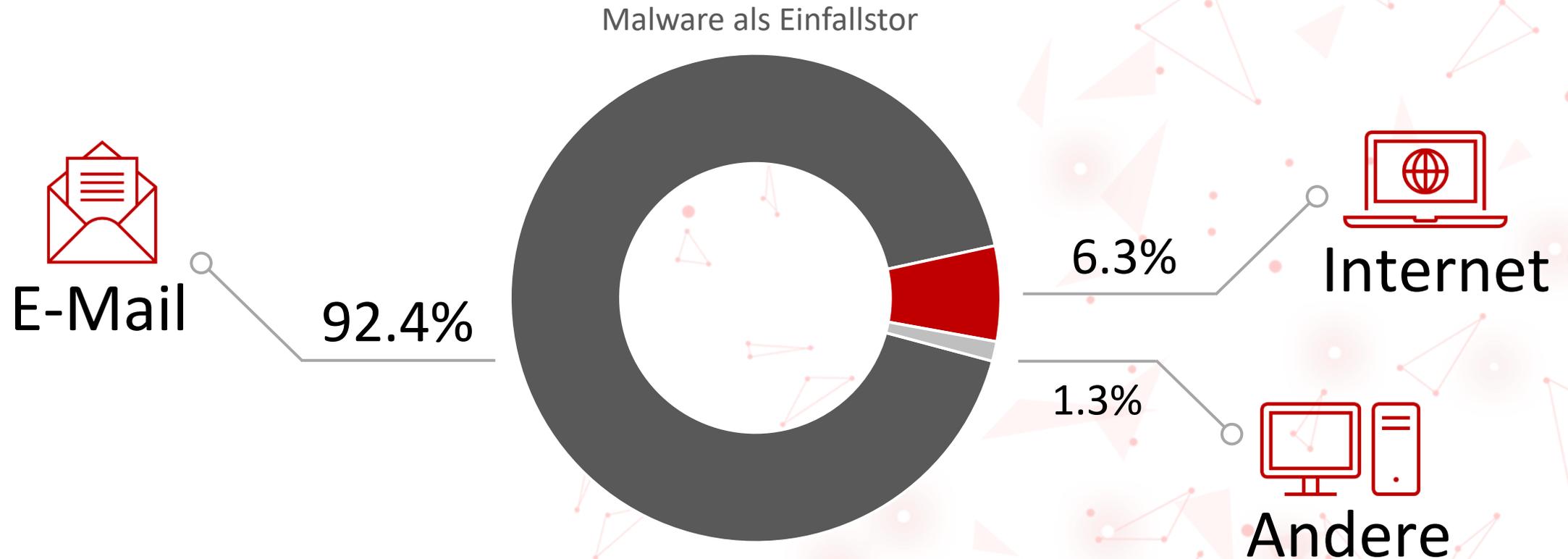
Staat & Verwaltung



Ransomware

Schwachstellen, offene oder falsch konfigurierte Online-Server

APT



15 Millionen

Meldungen zu Schadprogramm-Infektionen in Deutschland, übermittelte das BSI an deutsche Netzbetreiber.

207 Tage

Erster digitaler Katastrophenfall in Deutschland

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

117 Millionen zugenommen.

69% aller Spam-Mails waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.

Postbote > Postkarte

FASANA

Ransomware-Angriff am 19. Mai 2025

Ransomware

Fasana stellt Insolvenzantrag nach Cyberangriff

24.06.2025 · Von [Melanie Staudacher](#) · 2 min Lesedauer · 

Der Serviettenhersteller Fasana erlitt einen Ransomware-Angriff. Weil daraufhin nicht mehr produziert werden konnte, meldete das Unternehmen Insolvenz an. Fasana sucht nun nach einem Käufer, damit die rund 240 Stellen gerettet werden können.

Quelle: <https://www.security-insider.de/>

Es ist nicht die Frage, ob es passiert, sondern wann es passiert!

E-Mail Sicherheit



- * TLS-Verschlüsselung oder auch Transport-Verschlüsselung genannt
 - * Verschlüsselung zwischen Mail-Servern, z.B. OnPrem Exchange <> M365 Cloud Exchange
 - * Standard aktuell 1.3
- * Einsatz einer Mail-Gateway-Lösung
 - * Schutz vor Spam und Schadcode
 - * E-Mail Verschlüsselung und Signierung oder Umwandlung in Passwort geschütztes PDF
 - * URL-Filterung
 - * Meta Daten Analyse
 - * Mehrwertfunktionen, z.B. einheitliche oder zeitgesteuerte Disclaimer sowie gesonderte Übertragung und Behandlung von Dateianhängen
- * Durch die Gateway Funktionalität profitieren alle Teilnehmer
- * Einsatz zertifizierter Lösungen
- * Einsatz von Lösungen aus deutscher oder europäischer Entwicklung

SecurITy
made
in
Germany



- ✓ Einsatz einer Mail-Gateway-Lösung
 - ✓ Schutz vor Spam und Schadcode
 - ✓ Aufbau einer Vertrauensstellung und Kommunikationsbeziehung (Level of Trust)
 - ✓ Absenderreputation > eindeutige Feststellung des Absenders
 - ✓ SPF == Sender Policy Framework (DNS Eintrag welcher Server darf mit Domain versenden)
 - ✓ DKIM == DomainKeys Identified Mail (Absenderüberprüfung, Nachrichtenintegrität durch Signatur)
 - ✓ DMARC == Domain-based Message Authentication, Reporting & Conformance (SPF+DKIM+RL)
 - ✓ DANE == DNS-based Authentication of Named Entities (Server Authentizität mithilfe DNS-Einträgen)
 - ✓ ARC == Authenticated Received Chain (öffentliche Checkliste für Legitimität, Authentizität und Integrität von E-Mails einer Domain)
 - ✓ Mail-Flow basierend auf einem granularen Regelwerk
 - ✓ Intelligente Inhaltsfilterung (Schlagworte, Dateitypen, MIME-Typen, u.a.)
 - ✓ Schadcode Erkennung auch mittels Sandbox
 - ✓ Intelligente Meta Daten Analyse > Schwarm-Wissen, aber DSGVO konform
 - ✓ Möglichst keine Quarantäne > Abwehren statt Sortieren
 - ✓ URL-Filterung > Bewertung von URLs in E-Mails > bösartige werden entfernt, unsichere isoliert
 - ✓ Umwandlung schädlicher oder unsicherer Anhänge > Content Disarm & Reconstruction (CDR)

- ✓ Einsatz einer Mail-Gateway-Lösung
 - ✓ E-Mail Verschlüsselung und Signierung oder Umwandlung in Passwort geschütztes PDF
 - ✓ Unverschlüsselt > Postkarte
 - ✓ Einfach am Gateway ohne Einwirken der User
 - ✓ Zentrale & automatisierte Zertifikatsverwaltung
 - ✓ Schutz vor Industriespionage
 - ✓ DSGVO fordert: Schutz personenbezogener Daten
 - ✓ Häufige Voraussetzung für partnerschaftliche Zusammenarbeit
 - ✓ PGP Verschlüsselung oder S/MIME Zertifikate (Standard 4.0)
 - ✓ Hinterlegen der öffentlichen Schlüssel



Geben Sie eine E-Mail-Adresse ein, um nach einem passenden Zertifikat oder PGP-Schlüssel zu suchen.

Was macht eigentlich Microsoft?

#ITklugesichert

	Microsoft 365 + EOP	Microsoft Defender for Office 365	XYZ
DSGVO	Keine zentrale S/MIME Unterstützung		✓
Quarantäne unbegrenzt	–	–	✓
Wirkungsvoller Phishing-Schutz/ CxO-Fraud	–	(✓)	✓
Content Disarm & Reconstruction	–	–	✓
Nachrichten- verfolgung	(✓)	–	✓
Automatisierte Zertifikatsverwaltung	–	–	✓
Disclaimer- Management	–	(✓)	✓

„Menschen vor Bedrohungen ihres digitalen Arbeitsumfelds zu schützen und ihnen eine sichere und mühelose Kommunikation zu ermöglichen.“

Haben Sie Fragen?

**Besuchen Sie uns
auf Stand #20**

solutionIT

