



BMF

**BUNDESMINISTERIUM
FÜR FINANZEN**

Mag. Wolfgang Ebner

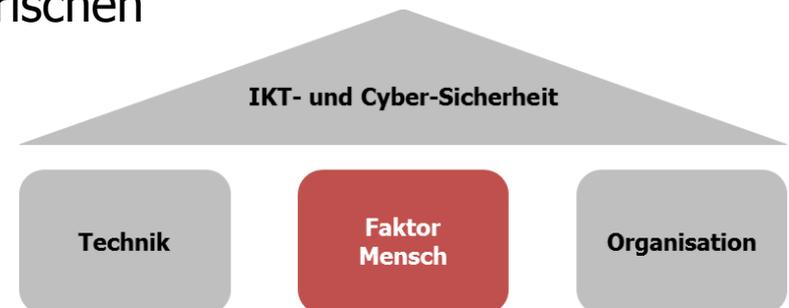
IKT-Sicherheitsportal

**Internetportal zur Förderung und Stärkung
der IKT- und Cyber-Sicherheit in Österreich**



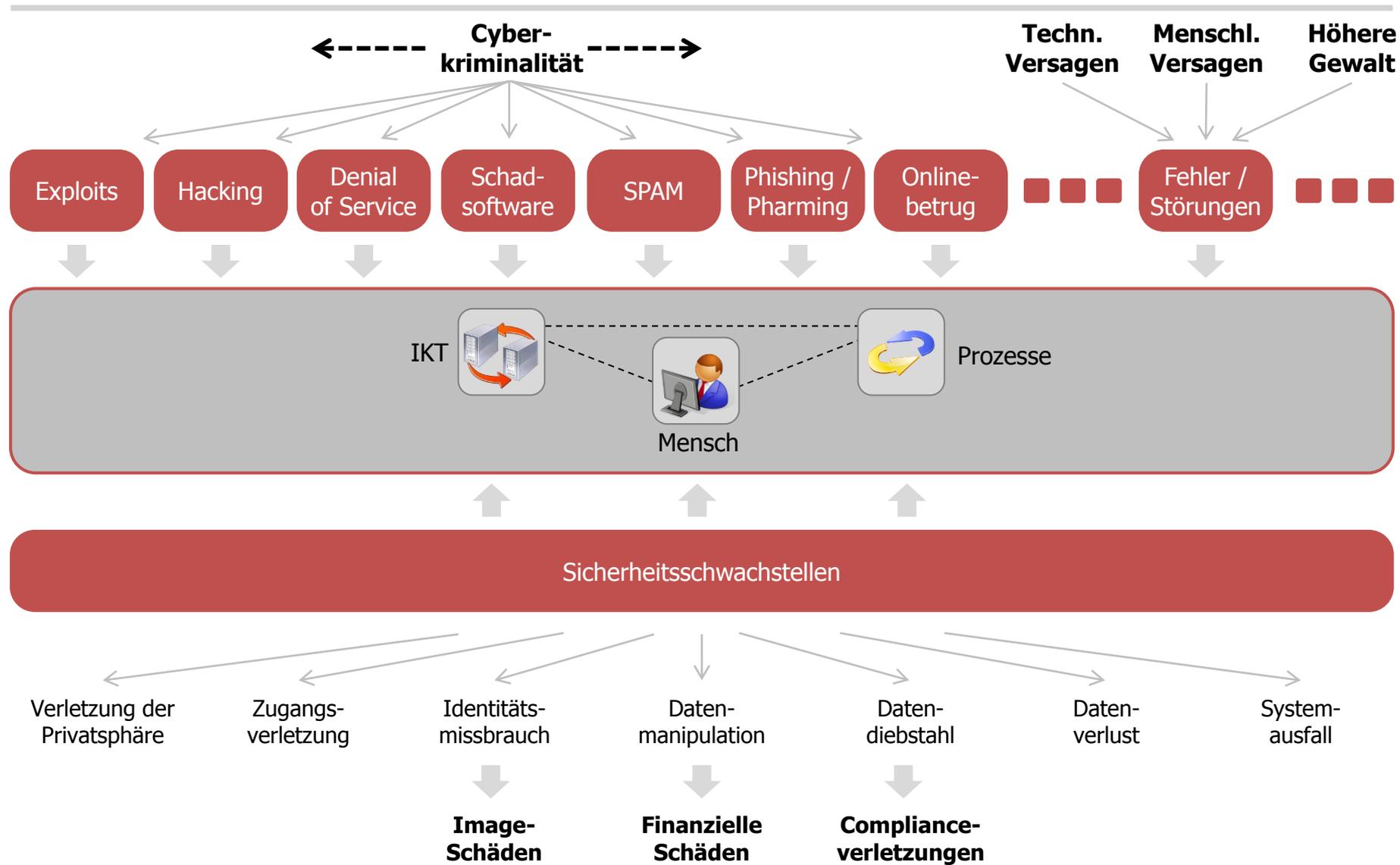
- Strategische Maßnahme der **Nationalen IKT-Sicherheitsstrategie** und der **Österreichischen Strategie für Cyber Sicherheit**
- **Interministerielle Initiative** in Kooperation mit der **österreichischen Wirtschaft**
- Internetportal, das sich ausschließlich der **IKT- und Cyber-Sicherheit** widmet
- Adressiert **alle betroffenen Zielgruppen und Sektoren** und unterstützt **Einsteiger/innen und Expert/innen**
- Dient der Förderung und nachhaltigen Stärkung der **IKT- und Cyber-Sicherheitskultur** in Österreich

- **Informations- und Kommunikationstechnologie (IKT)**
 - ist zu einer unverzichtbaren Grundlage geworden, wenn es um die Effizienz interner Geschäftsprozesse geht
 - bringt jedoch nicht nur neue Möglichkeiten und Spielraum, sondern schafft auch neue Abhängigkeiten und Sicherheitsrisiken
- **Österreichs Wirtschaft**
 - ist Teil einer digitalisierten und vernetzten Welt und benötigt daher ein angemessenes Sicherheitsniveau
- **Eine zukunftsorientierte IKT-Sicherheit**
 - muss neben technischen und organisatorischen Aspekten verstärkt den Faktor Mensch berücksichtigen



IKT-Sicherheitsportal

Ein Blick auf die aktuelle Bedrohungslandschaft



...vereinfachte Darstellung!

Sicherheitsschwachstellen in Softwareprodukten

zählen zu den größten Gefährdungen, da sie das Einfallstor für wesentliche Bedrohungen wie Schadprogramme und Hacker-Angriffe darstellen

- **Volumen**

- 2014 wurden über 7.900 neue Schwachstellen in Softwareprodukten verschiedenster Hersteller bekannt. Das entspricht einem Anstieg von über 50 Prozent zum Vorjahr.

- **Kritikalität**

- Etwa ein Viertel der Schwachstellen waren kritisch und erforderten eine rasche Behebung.

Quelle: National Institute of Standards and Technology (US)

Schadsoftware und Infektionen

Computer, die dem Schadsoftware-Ökosystem Internet ausgesetzt sind, stoßen früher oder später auch auf Schadprogramme wie Viren, Würmer und Trojaner

- **Volumen**

- Im dritten Quartal 2014 wurden weltweit über 40 Millionen neue Schadprogramme entdeckt. Das entspricht einem Anstieg von über 25 Prozent zum zweiten Quartal.

- **Begegnungsrate**

- Die Wahrscheinlichkeit tatsächlich auf Schadsoftware zu stoßen lag weltweit bei rund 20 Prozent.

Quellen: McAfee Labs Threats Report, Nov. 2014 / Microsoft Security Intelligence Report, Vol. 17

Alle betroffenen Zielgruppen und Sektoren



Sensibilisierung & Bewusstseinsbildung
Beratung & Unterstützung



Zielgruppenspez. Handlungsempfehlungen
Aktuelles



**Kooperations-
partner**

Redaktionelle
Beiträge
↔
Verlinkung
Content-Syndication

ONLINE SICHERHEIT.AT



News
↔
Verlinkung



**Internet-
Webseiten**

Betrieb und
Weiterentwicklung
↑
Portalredaktion und
Redaktionsgremien

- **Initiatoren & Auftraggeber**
 - Bundesministerium für Finanzen
 - Bundeskanzleramt
 - A-SIT Zentrum für sichere Informationstechnologie – Austria

- **38 Kooperationspartner**
 - Bundesministerien
 - Landesregierungen
 - Behörden
 - Universitäten, Fachhochschulen und Forschungsinstitute
 - Unternehmen, Vereine und Interessensvertretungen

Anwender/innen

Kinder &
Jugendliche

Eltern

Lehrende

Konsument/
innen

Generation
60plus

Mitarbeiter/
innen

Entwickler/innen und Betreiber/innen

Unternehmer/
innen

Öffentliche
Verwaltung

Sicherheits-
forschung

Stakeholder nationaler Initiativen

Nationale
Sicherheitsinitiativen

Unternehmer/innen

Sicherheitsmanagement

Sicherheitshandbücher

Sicherheitsnormen

Weitere Normen und Standards

Rechtliche Vorgaben

Industrielle Sicherheit

E-Government

E-Business-Statistik

Rat und Hilfe

- **Was sollte ein effektives Sicherheitsmanagement abdecken?**
- **Wie helfen Sicherheitshandbücher bei der Implementierung und beim Betrieb?**
- **Welche Sicherheitsnormen und -standards gilt es zu berücksichtigen?**
- **Welche rechtlichen Vorgaben sind einzuhalten?**
- **Was ist bei internationalen Aufträgen mit klassifizierten Informationen erforderlich?**
- **Wo finden sich weiterführende Informationen, Tipps und Hilfestellung?**

Mitarbeiter/innen

Computer- und Datensicherheit

Passwort-Sicherheit

Internet-Sicherheit

E-Mail-Sicherheit

Gefährliche Schadprogramme

E-Government

Rat und Hilfe



- **Was ist beim sicheren Umgang mit Computern und Informationen zu berücksichtigen?**
- **Was ist bei der Auswahl und Verwaltung von Passwörtern zu beachten?**
- **Welche Gefahren bestehen beim Surfen im Internet?**
- **Was gilt es im Umgang mit E-Mail und SPAM zu beachten?**
- **Wie können Schadsoftware-Infektionen verhindert werden und was ist zu tun, wenn es doch dazu kommt?**
- **Wo finden sich weiterführende Informationen, Tipps und Hilfestellung?**

Informatives

News

Publikationen

Veranstaltungen

Aktuelle Warnungen

Cybermonitor

Sicherheitswarnungen

Beratung

Online Ratgeber

Sicherheitshandbuch

Weiterführende Informationen

**Behörden &
Institutionen**

Cybermonitor

SPAM
Internetbetrug
Phishing
Identitätsdiebstahl
Schadsoftware
Infektionen
Exploits
Schwachstellen
Denial of Service
Störfälle
Hacking
Datenlecks
Spear Phishing
Spionage
Cybercrime

Cybermonitor

Die bestehenden Sicherheitsrisiken in der digitalen Welt sind vielfältig und oft nur schwer einschätzbar. Der Cybermonitor informiert über aktuelle Gefährdungstrends.

Zahlen und Fakten zu:

- **Schwachstellen und Bedrohungen**
- **Angriffszielen und Methoden**
- **Volumen und Kritikalität**
- **Vorfällen und Auswirkungen**
- **Betroffenen Sektoren, Produkten und Daten**



Online Ratgeber

IT-Sicherheit für EPU

Sicherheit der IT-Infrastruktur

Smartphone-Sicherheit

Facebook-Sicherheit



IT-Sicherheit für Ein-Personen-Unternehmen

Der Online Ratgeber zeigt einfache und rasch umzusetzende Maßnahmen für mehr IT-Sicherheit.

Die wichtigsten Themen:

- **Verfügbarkeits- und Datenverlust**
- **Vermeidung des Verlusts von Ansehen und Kundenvertrauen**
- **Datensicherung**
- **Passwörter und technische Sicherheit**

Online Ratgeber

IT-Sicherheit für EPU

Sicherheit der IT-Infrastruktur

Smartphone-Sicherheit

Facebook-Sicherheit

Sicherheit der IT-Infrastruktur

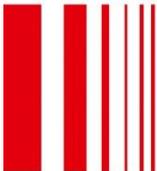
Der Online-Ratgeber unterstützt Unternehmen bei der Erfassung, Evaluierung und Reduzierung von Risiken beim Betrieb komplexer IT-Anwendungen.

BUNDESKANZLERAMT  ÖSTERREICH

Die wichtigsten Themen:

- **Identifizierung betrieblicher IT-Risiken**
- **Umsetzung von Maßnahmen zur Risikoreduzierung**
- **Implementierung reaktiver Maßnahmen bei Sicherheitsvorfällen**



 **ONLINE
SICHERHEIT.AT**



**Internetportal zur Förderung und Stärkung
der IKT- und Cyber-Sicherheit in Österreich**

www.onlinesicherheit.gv.at