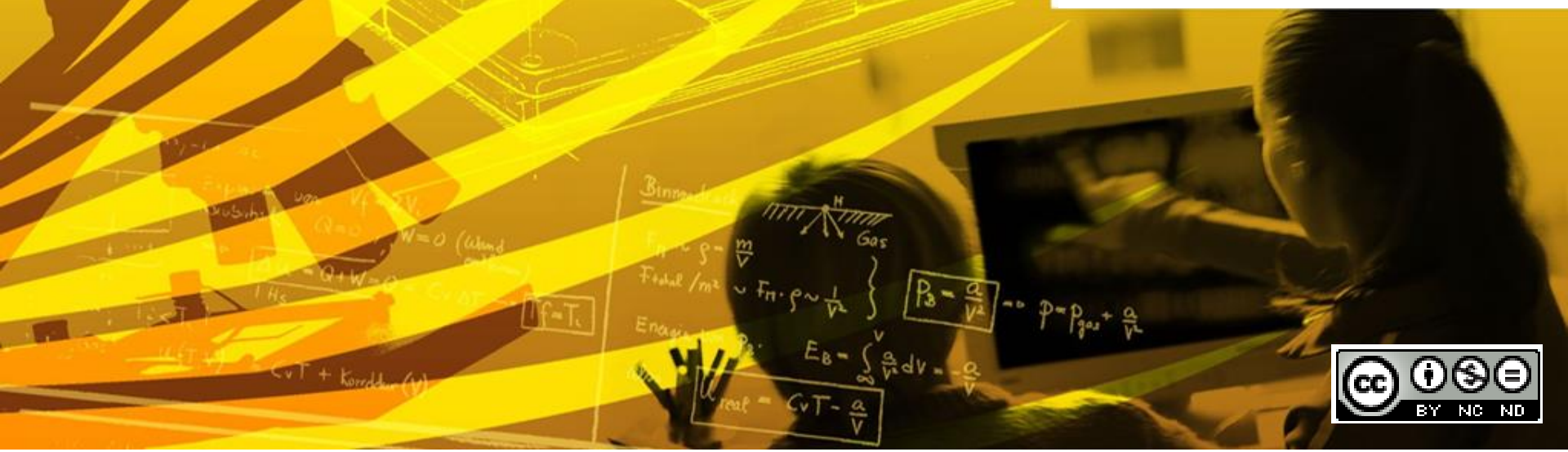
IT-Sicherheit

Abteilung IT/2
Informationstechnologie

Dr. Robert Kristöfl



BM BF Bundesministerium für Bildung und Frauen

efit 21

Begriffsdefinitionen

- **Safety / Funktionssicherheit:**
  stellt sicher, dass sich ein IT-System konform zur erwarteten Funktionalität verhält und einen störungsfreien Betrieb gewährleistet

- **Security / Informationssicherheit**:
  dient dem Schutz vor Gefahren, der Minimierung von Risiken und der Vermeidung von Schäden

Begriffsdefinition BSI

BSI (Bundesamt für Sicherheit in der Informationstechnik):

- **IT-Sicherheit** ist der Zustand, in dem **Vertraulichkeit, Integrität** und **Verfügbarkeit** von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

- **Informationssicherheit** ist umfassender als IT-Sicherheit und beinhaltet auch die Sicherheit von nicht elektronisch verarbeiteten Informationen

IT-Sicherheitsbereiche und -komponenten

- **Computer- und Datensicherheit:** Virenschutz, Zugriffs- und Rechtemanagement, Passwörter, **Identitätsmanagement**, Digitale Signaturen, Verschlüsselung, MDM (Mobile Device Management für Smartphones, Phablets, Tablets), etc

- **Netzwerksicherheit**: Firewall (Personal/Web Application Firewall), VPN (virtual private network), WLAN-Sicherheit, Authentifizierungs-mechanismen/Zertifkate, **Next Generation Firewall, Software-defined-networking,** etc.

- **Datensicherung und Notfallvorsorge:** Backup, Aufbewahrung Backup-Datenträger, Notfallwiederherstellung, etc.

- **Bauliche und infrastrukturelle Maßnahmen:** Zutrittskontrollen, unterbrechungsfreie Stromversorgung (USV), Brandschutz, Klimatisierung, etc.

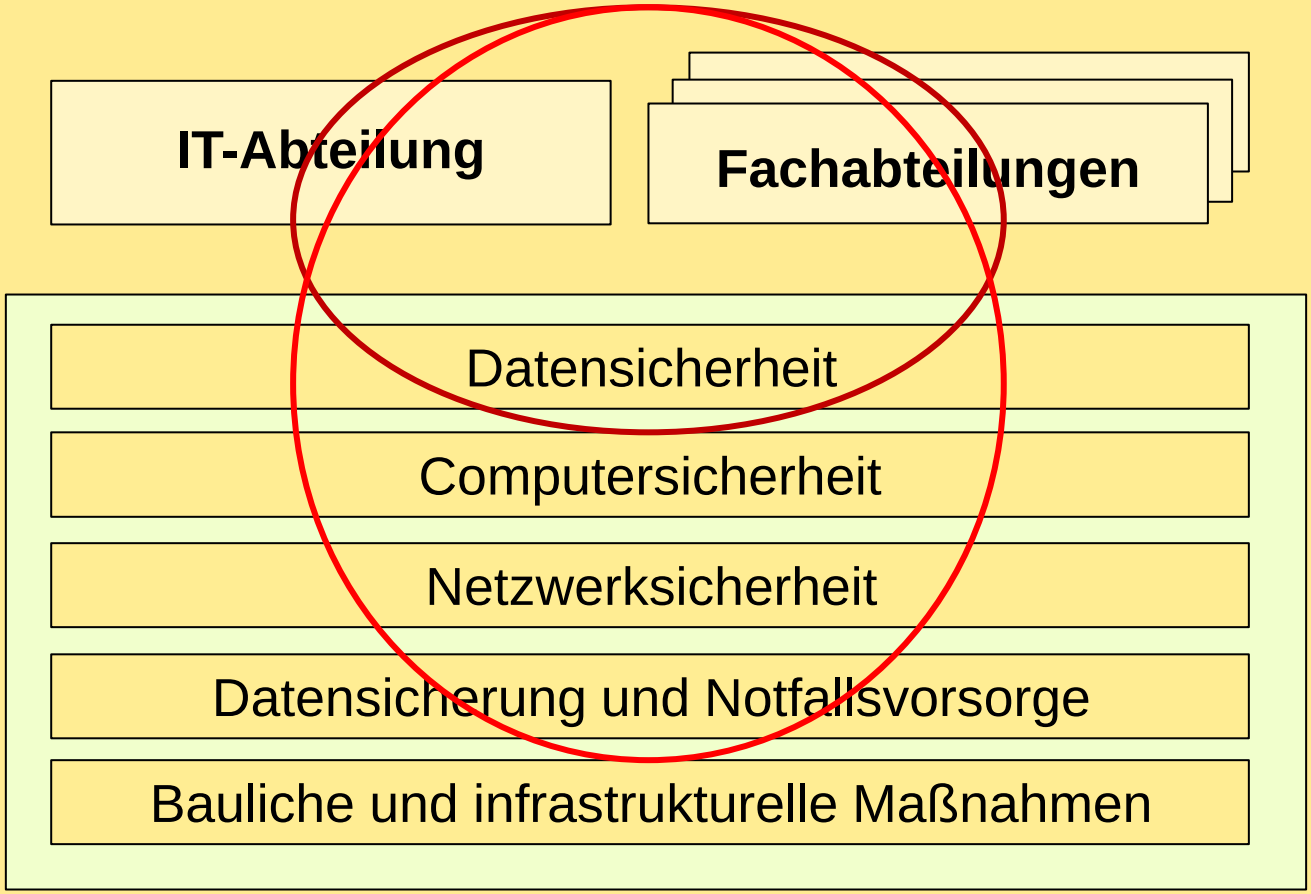
Kernziele der IT-Sicherheit

- **Vertraulichkeit (confidentiality)**: Daten dürfen lediglich von autorisierten Benutzern gelesen und modifiziert werden.
- **Integrität (integrity)**: Daten müssen unversehrt und korrekt bleiben und dürfen nicht unbemerkt verändert werden
- **Verfügbarkeit (availability)**
  Verhinderung von Systemausfällen; der Zugriff auf Informationen/Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.
- **Authentizität (authenticity):** bezeichnet die Eigenschaft der Echtheit, Überprüfbarkeit und Glaubwürdigkeit

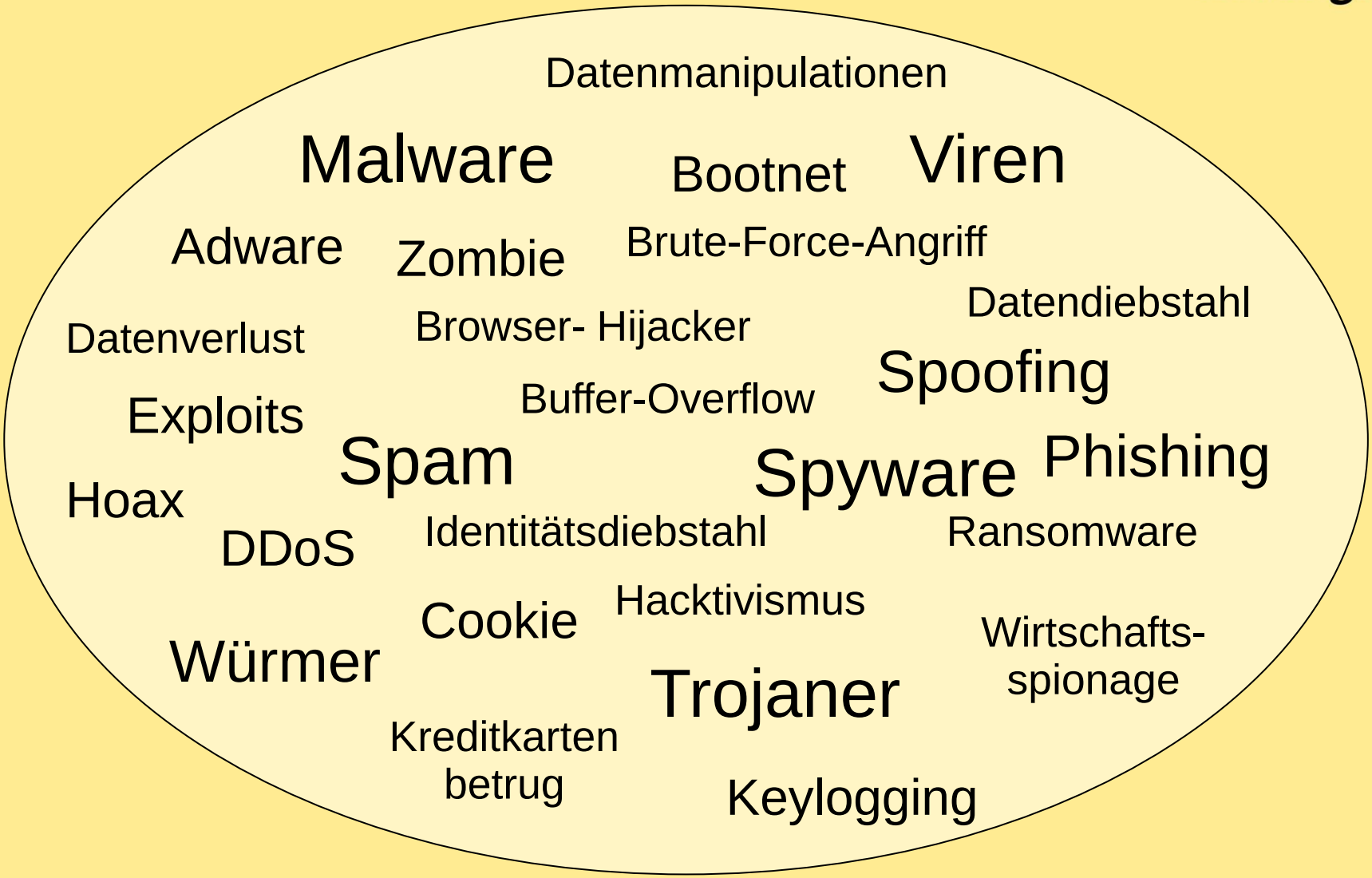
Verantwortlichkeit der IT-Sicherheit

bildung.at

Ist **IT-Sicherheit** Aufgabe der **IT-Abteilung?**

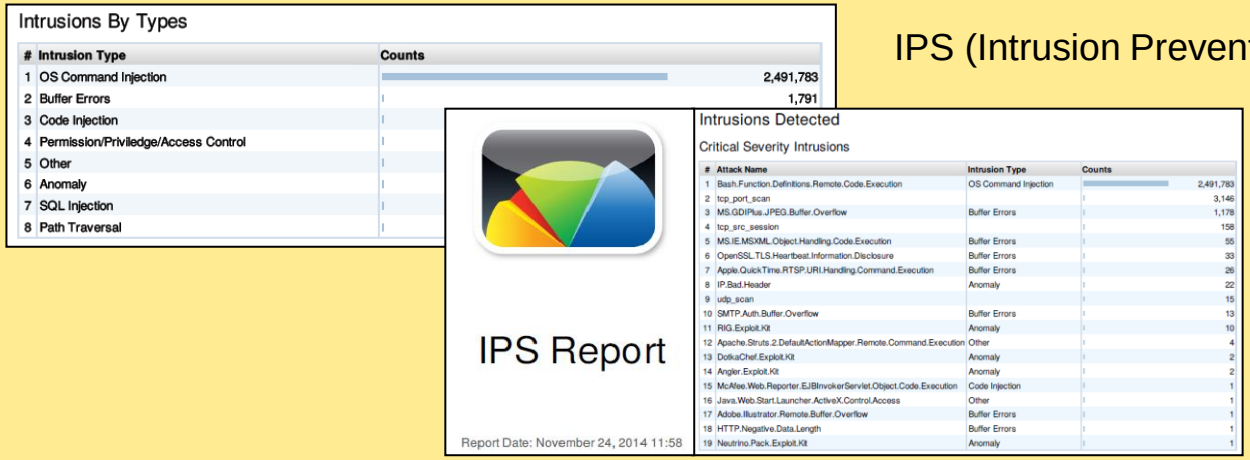


Bedrohungsszenarien



Bedrohungslage

- 1,8 Mio neue Computerschädlinge pro Halbjahr
- alle 8,6 Sekunden ein neuer Computerschädling für Windows-PCs und Notebooks
- 2,5 Mio Sicherheitsattacken im BMBF Rechenzentrum pro Monat
- mehr als 80.000 Sicherheitsattacken pro Tag, 3.480 pro Stunde, 58 pro Minute



Intrusions By Types

#	Intrusion Type	Counts
1	OS Command Injection	2,491,783
2	Buffer Errors	1,791
3	Code Injection	
4	Permission/Priviledge/Access Control	
5	Other	
6	Anomaly	
7	SQL Injection	
8	Path Traversal	

IPS Report

Report Date: November 24, 2014 11:58

Intrusions Detected

Critical Severity Intrusions

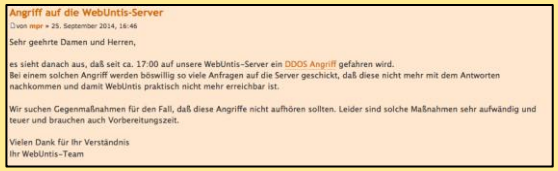
#	Attack Name	Intrusion Type	Counts
1	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	2,491,783
2	tcp_port_scan		3,146
3	MS.GDIPlus.JPEG.Buffer.Overflow	Buffer Errors	1,178
4	tcp_src_session		158
5	MS.IE.MSXML.Object.Handling.Code.Execution	Buffer Errors	55
6	OpenSSL.TLS.Heartbeat.Information.Disclosure	Buffer Errors	33
7	Apple.QuickTime.RTSP.URI.Handling.Command.Execution	Buffer Errors	26
8	IP.Bad.Header	Anomaly	22
9	udp_scan		15
10	SMTP.Auth.Buffer.Overflow	Buffer Errors	13
11	RIG.Exploit.Kit	Anomaly	10
12	Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	Other	4
13	DotkaChef.Exploit.Kit	Anomaly	2
14	Angler.Exploit.Kit	Anomaly	2
15	McAfee.Web.Reporter.EJBInvokerServlet.Object.Code.Execution	Code Injection	1
16	Java.Web.Start.Launcher.ActiveX.Control.Access	Other	1
17	Adobe.Illustrator.Remote.Buffer.Overflow	Buffer Errors	1
18	HTTP.Negative.Data.Length	Buffer Errors	1
19	Neutrino.Pack.Exploit.Kit	Anomaly	1

IPS (Intrusion Prevention System)

Sicherheits-Vorfälle im BMBF-Umfeld

bildung.at

- BIFIE Datenleck, Februar 2014
- „Heartbleed“-Lücke, April 2014



- DDoS Attacke WebUntis, September 2014
- Datenleck an Salzburg HAK, Oktober 2014
- DoS Attacke auf BMBF- Applikation, März 2015

- Defacement auf BMBF- Webauftritt, März 2015
- DDoS Attacke WebUntis, April 2015
- DoS Attacke auf BMBF- Applikation, September 2015

Austrian Vulnerability Report 2015

www.first-security.com

- Überprüfung von 13 Millionen IP-Adressen in Österreich auf potentielle Schwachstellen
- 1.600 Systeme im Einsatz, für die es keine Sicherheits-Updates mehr gibt: Windows XP, 98, 2000 und NT
- Windows XP, Vista, 2000 und 2003 bieten ein großes Angriffspotential mit einer sehr hohen Anzahl an Schwachstellen, die Schwachstellen erhöhen sich um 20% pro Jahr
- 70% der Schwachstellen befinden bei Webdiensten (http-Server - Port 80 und https-Server – Port 443)

IT-Sicherheits-Management und Risikoanalyse

- Eingerichtete **Frühwarnsysteme** Cert, GovCert, AcoNet-Cert
- Analyse und Erhebung von Schwachstellen und Bedrohungen
- Webauftritte/Anwendungen nach Risikostufe klassifizieren
- Planung und Umsetzung von durchgängigen **Sicherheitsmaßnahmen**
- Sicherheitspolicy für **Mobile Computing** und **Cloud Services**
- Regelmäßige **Vulnerability-Scans** und **Security Monitoring**
- Schuladäquate **Mustervereinbarungen** und Vorgaben auf Basis des **Datenschutzgesetzes** (DSG 2000) und Cybersecurity-Handbuch

IT-Sicherheits-Maßnahmen

- Regelmäßige **Software-Updates** – unterstützt durch Software-Verteilungslösungen und **Patch-Management**
- Richtige Konfiguration der **Firewalls**, Ergänzung durch Application Firewalls (Planung Next Generation Firewall)
- Benutzerrechte (eingeschränkte privilegierte Rechte) und keine einfachen Passwörter (zeitliche Gültigkeit, one time password, 2-Faktoren-Authentifizierung)
- Verschlüsselung sensitiver Informationen
- Richtlinien und Regelungen für MitarbeiterInnen
- Sicherheitssensibilisierung und Schulungsmaßnahmen für MitarbeiterInnen

Lessons Learned:

- IT-Sicherheit mit Maß und Ziel
- Schulungen über potentielle Gefahren sind sinnvoller als Verbote und Sperren

Vielen Dank für eure Aufmerksamkeit!

ABER: Menschen sind äußerst kreativ bei der Umgehung von Sicherheitsvorkehrungen