Bundesamt
für Sicherheit in der
Informationstechnik

Sources: The value of trustworthy and reliable Sources - Today

Lagebild
Cyber-Sicherheit

Federal Gov't Sources

- CS Situation Centre
- Federal gov't networks
- Registration Office

Bundesamt
für Sicherheit in der
Informationstechnik

Sources of ACS

- Partners of ACS
- Registered incidents

Allianz für
Cyber-Sicherheit

Other sources

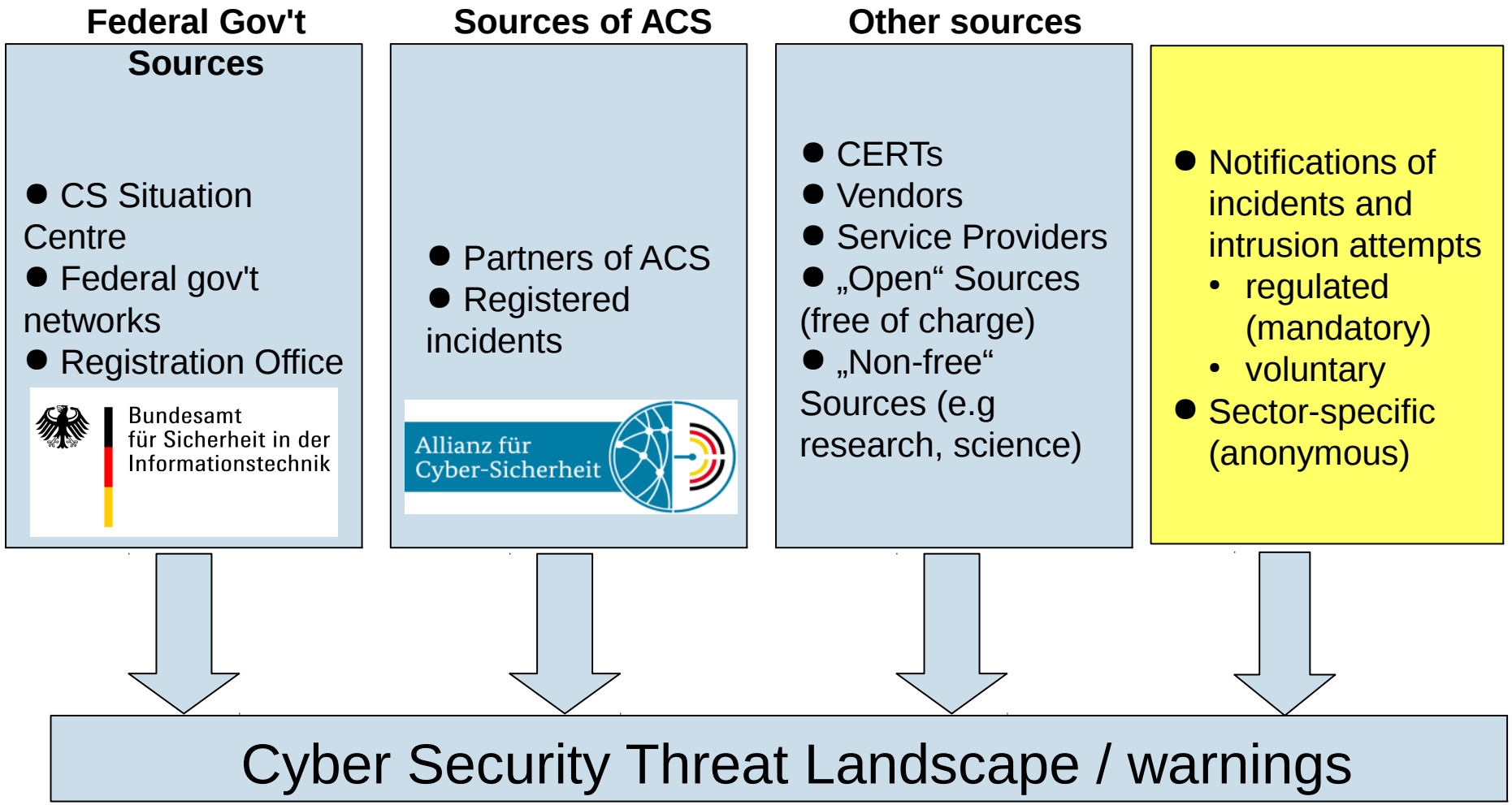
- CERTs
- Vendors
- Service Providers
- „Open“ Sources (free of charge)
- „Non-free“ Sources (e.g research, science)

Cyber Security Threat Landscape / warnings

Bundesamt
für Sicherheit in der
Informationstechnik

Sources: The value of trustworthy and reliable Sources - Tomorrow

Future additional Sources from ITSiG



Bundesamt
für Sicherheit in der
Informationstechnik

Envisaged Future Use of Threat Landscape Information

„Dynamic “ Cyber Security Threat Landscape

Kategorien der Bedrohungen und Schwachstellen

A Schadprogramme (Malware)	**E Physische Angriffe**	**I Organisatorische Mängel**
1 Malware-Infektion z. B. durch Trojaner, Rootkits, Backdoors, Spyware zum Zwecke der Kontrollübernahme, Datenmanipulation oder des Datenabflusses	1 Unbefugter Zutritt	1 Fehlende oder unzureichende Prozesse oder Regelungen zur IT-Sicherheit usw.
2 Angriffe durch Bots bzw. Botnetze z. B. DDoS-Angriff, Malware-Verteilung, Spam-Verteilung	2 Diebstahl, Verlust, Zerstörung oder unsachgemäße Aussonderung von mobilen Endgeräten	2 Ressourcenmangel oder Personalausfall z. B. fehlende Zuständigkeiten oder Vertreterregelungen
3 Ransomware z. B. Sperren von IT-Systemen zu Erpressungszwecken	3 Diebstahl, Verlust, Zerstörung oder unsachgemäße Aussonderung von IT-Komponenten	3 Unvollständiges Patch- und Änderungsmanagement
4 Adware, Scareware z. B. zu Betrugszwecken	**F Technisches Versagen**	4 Ungeeignetes oder fehlendes Passwortmanagement
5 Multifunktionale Schadprogramme z. B. Viren, Würmer, Riskware	1 Ausfall von IT-Systemen, Anwendungen oder Netzen z. B. Strom	5 Mangelnde Sensibilisierung und Schulung
6 Malware-Infektion mobiler Endgeräte z. B. durch bösartige Apps zum Zwecke der Manipulation bzw. Datendiebstahl	2 Verlust gespeicherter Daten z. B. defekte Speichermedien oder Datenträgern	6 Unzureichender Umgang bei Sicherheitsvorfällen bzw. fehlendes Notfallmanagement
B Hacking und Manipulationen	**G Höhere Gewalt**	7 Unzureichende Dokumentation
1 Webanwendungsbasierte Angriffe z. B. Drive-by-Exploits	1 Ausfall von Infrastrukturen z. B. Internet, Telefonnetzen	8 Unzureichendes Privacy Management z. B. in Sozialen Netzwerke
2 Angriffe auf Webanwendungen z. B. SQL-Injection, Buffer Overflow	2 Naturkatastrophen bzw. Umwelt z. B Hochwasser, Sturm	**II Systemschwachstelle (technisch)**
3 Angriffe auf Anwendungen bzw. Dienste wie DNS, SMTP, FTP	3 Terroristische Akte	1 Software-Schwachstellen oder Firmware-Schwachstellen
4 Systematisches Ausprobieren von Passwörtern	**H Verhinderung von Diensten**	2 HW-Schwachstellen
5 Missbrauch elektronischer Sendedienste z. B. Spam-E-Mails	1 Überflutung (z. B. DDoS durch Botnetze)	**III Menschliches Fehlverhalten (Personal)**
6 Spionage bzw. Abhören von Daten oder Informationen z. B durch fehlende oder schwache Verschlüsselung	2 Gezielter Systemabsturz z. B. Paketfragmentierung, Ausnutzung von Softwareschwachstellen	1 Konfigurationsfehler
7 Täuschen bzw. Verändern z. B. Spoofing, Poisoning	**I Identitätsmissbrauch**	2 Bedienfehler oder Wartungsfehler
8 Übernehmen von bestehenden Sitzungen z. B. Session Hijacking	1 Diebstahl von Zugangsdaten z. B. Identitätsdiebstahl, Phishing, Spear-Phishing, Pharming, Skimming	3 Designfehler bei der Planung
9 Manipulation von Hardware oder Software z. B. Lieferketten	2 Verschleierung einer Identität	4 Implementierungsfehler bei der Realisierung
C Social Engineering (nicht technisch)	3 Diebstahl oder Fälschung von Zertifikaten	**IV Infrastruktur**
1 Manipulation von Mitarbeitern zur Weitergabe falscher oder interner Informationen z. B. aus Gutgläubigkeit oder Angst	4 Unrechtmäßige Registrierung von Internetdomänen (Cybersquatting)	1 Bauliche Mängel z. B. durch fehlenden Brandschutz
2 Informationssammlung über Mitarbeiter z. B. über soziale Netzwerke, Dumpster Diving d.h. Müll durchwühlen	**J Abhängigkeit von Dienstleistern und Herstellern**	2 Unzureichende Dimensionierung der Infrastruktur z. B. Räume, Stromversorgung
3 Reverse Social Engineering z. B. Vortäuschen eines Vorfalls	1 Unkontrollierbarer Zugriff auf ausgelagerte Informationen, Software, Dienstleistungen	3 Unzureichende Klimatisierung
4 Rücksetzen fremder Passwörter über Hotlines (Mat-Honan-Hack)	2 Ausfall von Dienstleistern (Interdependenzprobleme) z. B. Ausfall von Cloud-Dienstleistern	**V Netze-/ Kommunikationsverbindungen**
D Missbrauch (Innentäter)	3 Hintertüren und versteckte Funktionen in Software und Geräten	1 Ungeeignete Sicherheitsarchitektur oder Netzmanagement
1 Weitergabe interner Informationen		2 Fehlende oder unzureichende Netzsegmentierung
2 Unberechtigtes Erlangen von besonderen Zugriffsrechten z. B. von Administrationsrechten		3 Verwendung unsicherer Protokolle oder Netze z. B. WLAN
3 Missbräuchliche Nutzung von Berechtigungen (insbesondere von Zugriffsrechten) z. B. durch Externe über Fernwartungszugängen		

Grau/Weiss ->Kategorien der Bedrohungen (Angriffsvektoren)
Gelb/Weiss-> Kategorien der Schwachstellen
(Version 1.2 Stand 08.09.2014)

„Dynamic“ list of top threats and vulerabilities

Prioritized recommendations for IT-security safeguards in the IT-Grundschutz catalogues

Links

- The State of IT Security in Germany 2014 (en)

https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html