GovCERT AUSTRIA

CERT.at

BERICHT INTERNET-SICHERHEIT ÖSTERREICH 2015

FACTSHEET

Wien, Februar 2016

(A) Globale Entwicklungen samt Zahlen und Daten

Industrie 4.0

- Die Deutsche Telekom sieht die Sicherheit als eines der größten Fragezeichen für die Industrie 4.0 in ihrem Cyber Security Report 2015.
    - In dem Bericht wird angeführt, dass in Deutschland 36% der Unternehmen mehrmals pro Woche Opfer von IT-Angriffen werden.
- Beim sogenannten Honeynet-Projekt analysierte die deutsche TÜV SÜD acht Monate lang Spähangriffe auf ein kleines Wasserwerk. Dabei konnten Attacken aus über 150 Ländern registriert werden, was ein deutliches Warnsignal darstellt.
- Beim Angriff auf einen Jeep Cherokee in den USA verschafften sich Angreifer über das Entertainment System Zugang zum Auto. In Folge dieser Attacke wurden 1,4 Millionen Fahrzeuge vom Hersteller zurückgerufen.

Cloud Dienste

- Laut dem amerikanischen Cloud Anbieter Salesforce nutzen weltweit bereits ein Drittel der Privatpersonen und 60% der Unternehmen Cloud Dienste.
- Zu den größten Risiken in der Cloud gehören unter anderem die Erfüllung von gesetzlichen Anforderungen in verschiedenen Ländern und Datendiebstahl.

Mobile Internetnutzung steigt

- Zu Beginn des Jahres 2015 wurden 31% aller weltweiten Internetaufrufe durch mobile Endgeräte getätigt (Quelle: Statcounter). Im Jahr 2014 waren dies noch 22%.
- Mobilgeräte werden vorwiegend für Online Einkäufe und soziale Netzwerke genutzt. Der hohe Anteil an persönlichen Daten in Mobilgeräten steigert deren Attraktivität für Cyber Attacken.

Cyber Angriffe als „Wirtschaftszweig"

- Heute reichen die Absichten der Angreifer von Aktivismus im Internet (sog. „Hacktivismus") über organisiertes Verbrechen mit dem Ziel eines finanziellen Profits bis hin zu staatlicher Spionage.
- Diese Vielfalt an Angriffsmotiven führte zu einem regelrechten Untergrundmarkt, auf dem millionenfach Daten zum Verkauf angeboten werden. Diesen Trend zeigen Publikationen wie der aktuelle McAfee Bericht „Das heimliche Geschäft mit Daten".

Unternehmen werden verstärkt zur Zielscheibe

- Kaspersky analysierte im Security Bulletin 2015/2016 Angriffsarten und kam zu dem Ergebnis, dass über die Hälfte der weltweiten Rechner in Unternehmensnetzwerken (58%) mindestens eine Malware Attacke 2015 zu überstehen hatten.
- Der 2015 Symantec Internet Security Threat Report greift auf 157 Länderdaten zurück.
    - Es wurden weltweit 2014 um 23% mehr Sicherheitslücken identifiziert als 2013.
- Angreifer machen sich Sicherheitslücken schneller zunutze, als Unternehmen entsprechende Patches bereitstellen können.

Sicherheitsbewusstsein in Europa muss geschärft werden

- Mit der im Februar 2015 veröffentlichten Eurobarometer-Umfrage zu Cyber Sicherheit fing die EU-Kommission die Perspektive der Bevölkerung ein.
- Mit über 150.000 Viren und über einer Million Opfern von Cyber Attacken pro Tag spielen Cyber Bedrohungen in der EU eine wesentliche Rolle.
- Die häufigsten Aktivitäten der europäischen NutzerInnen sind das Abrufen von E-Mails (86%), Lesen von Online Zeitungen (63%), soziale Netzwerke (60%) und Online Einkäufe (57%).
- Die Verhaltensweisen der User zeigt die Eurobarometerumfrage wie folgt:

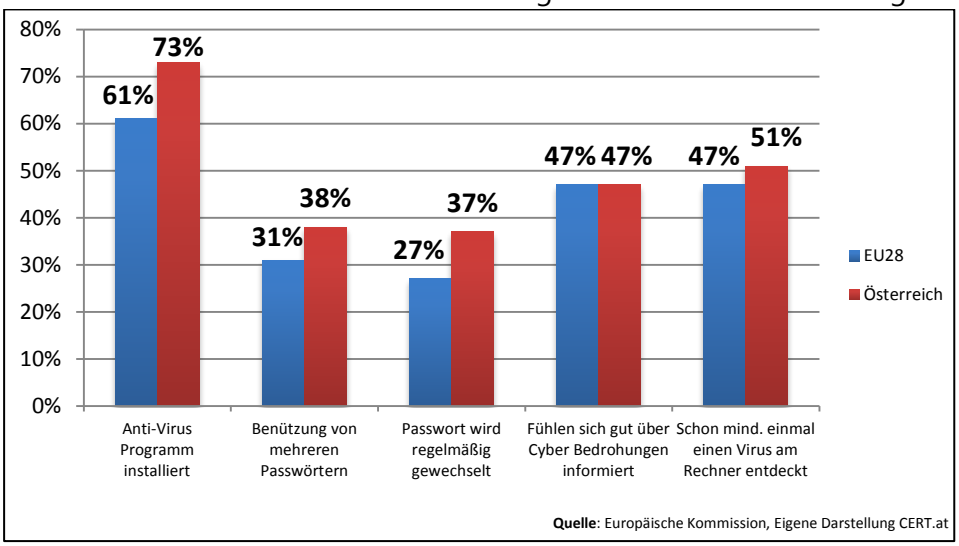


Abbildung: Ausgewählte Cyber Sicherheit Eurobarometer Umfrageergebnisse (EU28 & Österreich)

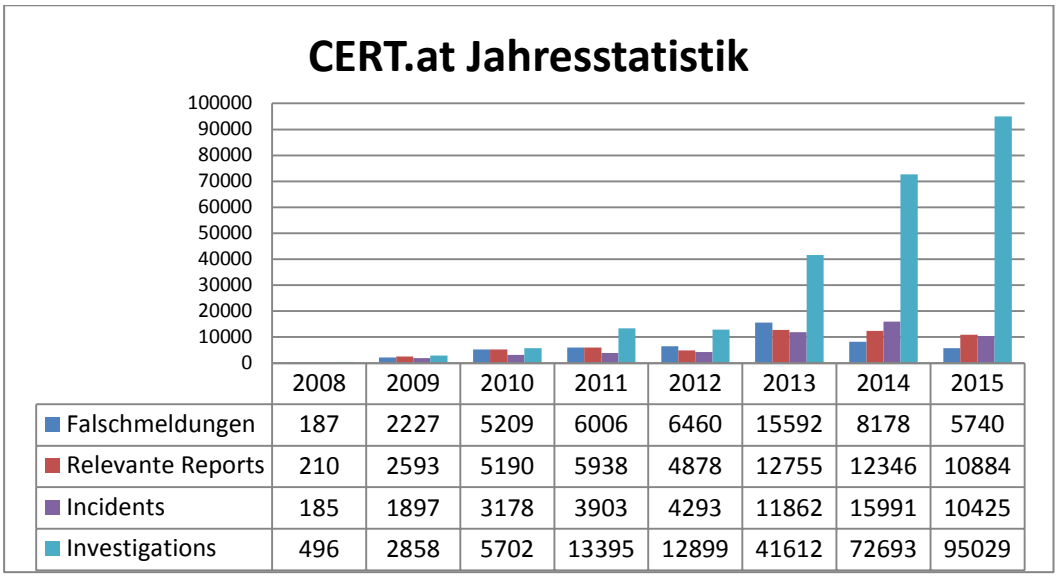
(B) DAS INTERNET-SICHERHEITSJAHR 2015 IN ÖSTERREICH

- CERT.at und GovCERT Austria führen umfangreiche Statistiken, mit denen sich ein Bild über die aktuelle Internet-Sicherheitslage Österreichs machen lässt. Wichtige Kennzahlen bei der vom CERT behandelten Vorfälle sind Reports, Incidents und Investigations.
- **„Reports"** bezeichnen eingehende Meldungen an CERT.at, welche nicht notwendigerweise gleich einen Incident bedeuten müssen.
- Als „**Incidents**" werden jene Fälle eingestuft, die tatsächlich ein Sicherheitsrisiko darstellen. Bei diesen schreitet CERT.at ein und informiert betroffene Unternehmen, Organisationen oder PrivatanwenderInnen über IT-Sicherheitsbedrohungen und unterstützt bei Bedarf bei der Problemlösung.
- Diese Kontaktaufnahme wird im CERT.at Ticketsystem als „**Investigation**" bezeichnet.

Wichtig: Bei der Interpretation der Grafiken und Statistiken ist zu beachten:

1. Eine Verbesserung in der Sensorik besitzt oft viel mehr Einfluss auf die Kurve, als eine Veränderung der dahinterliegenden Vorfälle. Wenn etwa durch eine Polizeiaktion in den USA plötzlich Daten zu einem Botnetz verfügbar werden, dann bedeutet dies einen plötzlichen und großen Sprung in den CERT.at Statistiken. In Wirklichkeit wurde das Botnetz aber über einen längeren Zeitraum hinweg aufgebaut.
2. Nicht alle Vorfälle sind gleichwertig relevant. So kann ein Incident sowohl ein fehlkonfigurierter Surf-PC in einer Jugendherberge sein, als auch ein Einbruch in einen Webshop mit dem Verlust tausender KundInnendaten.
3. Viele der Incidents behandeln bereits zusammengeführte Informationen. So etwa generiert die Sensorik zu falsch konfigurierten Nameservern einen Report pro Tag, unabhängig davon wie viele einzelne IP-Adressen enthalten sind. Die ausgehenden Mails an die Netzbetreiber können ebenfalls von einem einzelnen Vorfall bis hin zu einer langen Liste an betroffenen KundInnen reichen.

Die folgende Abbildung gibt einen Überblick über CERT.at Jahresstatistiken seit 2008. Sie beinhaltet die Zahl der Falschmeldungen, relevanten Reports, Incidents und Investigations:



	2008	2009	2010	2011	2012	2013	2014	2015
Falschmeldungen	187	2227	5209	6006	6460	15592	8178	5740
Relevante Reports	210	2593	5190	5938	4878	12755	12346	10884
Incidents	185	1897	3178	3903	4293	11862	15991	10425
Investigations	496	2858	5702	13395	12899	41612	72693	95029

Abbildung: CERT.at Jahresstatistik mit Übersicht über Reports, Incidents und Investigations im Zeitverlauf, Quelle: CERT.at

In der folgenden Abbildung werden die relevanten Reports an CERT.at im Zeitverlauf des letzten Jahres dargestellt. Dabei wird die Anzahl der relevanten Meldungen pro Monat in den Top 15 Kategorien wiedergegeben:

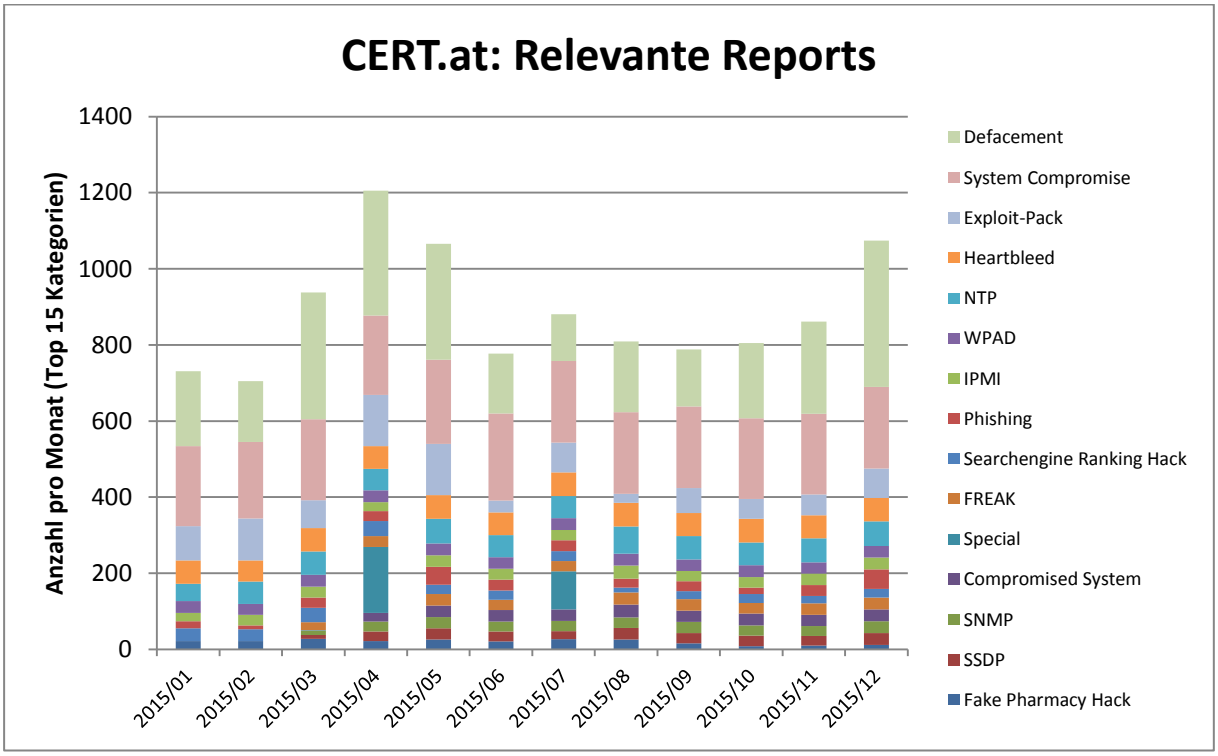


Abbildung: Klassifizierung der relevanten Reports nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

Die Zahl der Fälle, die tatsächlich ein Sicherheitsrisiko darstellten („Incidents“), finden sich in der folgenden Abbildung:

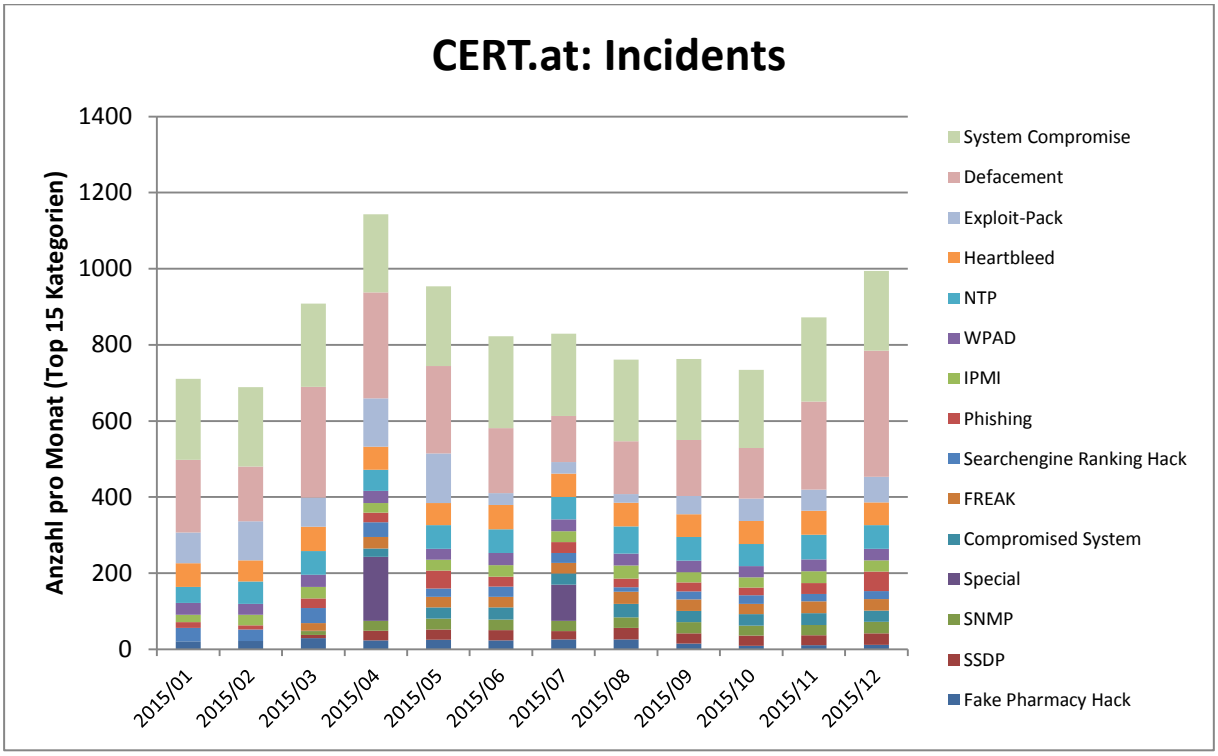


Abbildung: Klassifizierung von Incidents nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

Die Zahl der Investigations, also die Kontaktaufnahmen mit betroffenen Unternehmen, Organisationen oder PrivatanwenderInnen, behandelt die folgende Abbildung:

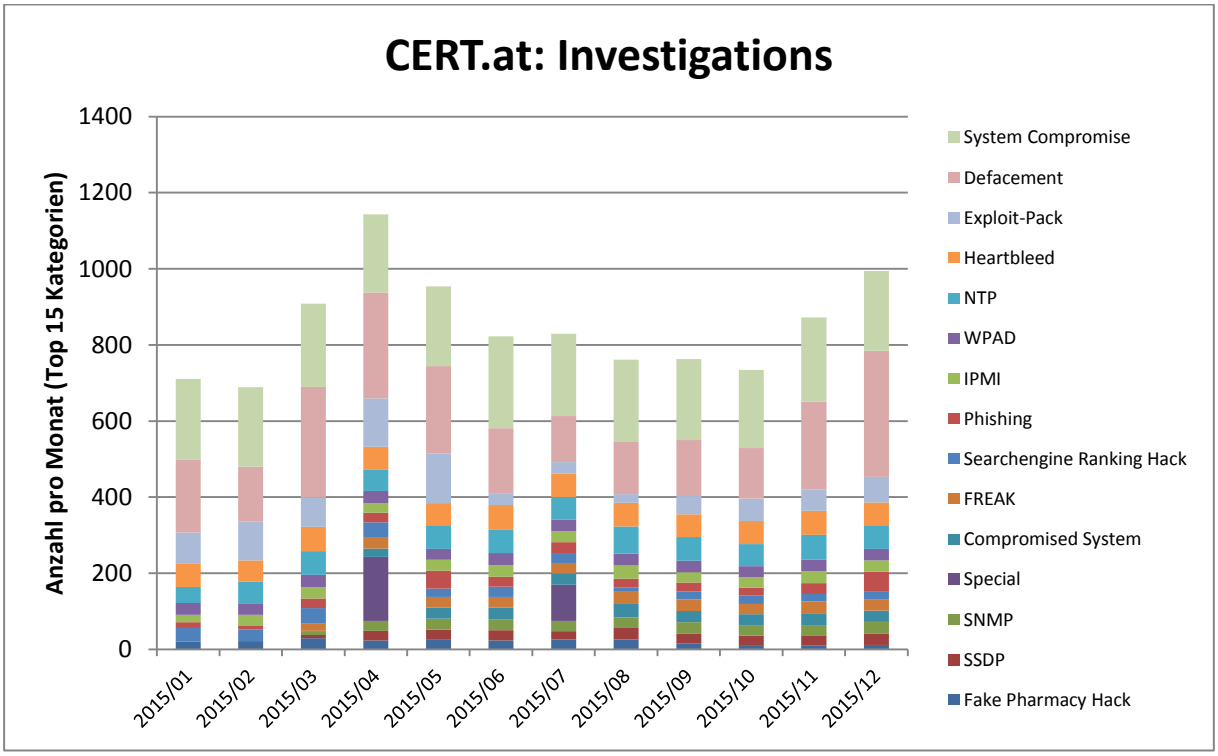


Abbildung: Klassifizierung der von CERT.at durchgeführten Investigations nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

Immer mehr Unternehmen auch in Österreich von Angriffen betroffen

- Wie es um die IT-Sicherheit in österreichischen Unternehmen bestellt ist, hat SORA im Auftrag von A1 unter die Lupe genommen.
  - Ein Drittel der befragten Unternehmen musste bereits auf Schadensfälle reagieren.
  - 80% hatten mit Beeinträchtigungen ihrer Systeme zu kämpfen.
  - Den häufigsten Bedrohungen – Schadsoftware, technische Probleme wie Netzwerkausfälle und Angriffe von Hackern – wird mit laufender Wartung, Updates und Schulungen entgegen getreten.
  - 95% der Unternehmen setzen auf Anti-Virus und Anti-Malware Software, jedoch verwenden nur 86% eine Firewall.
  - Mobile Endgeräte werden nur von 38% der Befragten geschützt.

Verschlüsselung bleibt weiter ein Thema

- Immer mehr Mailserver verwenden Transportverschlüsselung – Von weltweit 33% im Jahr 2013 auf 61% im Jahr 2015 ist diese Entwicklung durchaus positiv zu sehen.
- Gegen Ende 2014 zeichneten sich jedoch schon Probleme bei Verschlüsselungen ab - Stichwort POODLE (Padding Oracle On Downgraded Legacy Encryption) und „FREAK".
- Den Zahlen nach, die CERT.at vorliegen, läuft noch auf rund 600 IP-Adressen ein Webserver, der für diesen Angriff anfällig ist.

Vorsicht vor gefälschten Rechnungen

- Eine weitere Entwicklung, die auch zahlreiche ÖsterreicherInnen betrifft, ist die Verlagerung von Betrugsmaschen (Vorschussbetrug, Neffentrick oder der Versuch, mit gefälschten Rechnungen an Geld zu gelangen) in das Internet.
- Regelmäßig sind auch große Online Unternehmen wie Amazon & Co. von in Umlauf gebrachten gefälschten Rechnungen betroffen.
- Außerdem sind u.a. auch E-Mails von Paketdienstleistern, Mobilfunkanbietern oder Banken im Umlauf. Über die E-Mails, die für Laien schwer von Originalmails zu unterscheiden sind, wird versucht, die User auf Webseiten zu locken, die diverse Schadsoftware verbreiten.
- Ende 2014 und Anfang 2015 wurden diverse Industriebetriebe in Österreich Opfer des **Spoofed Invoice Frauds**.
    - Es entstanden u.a. Schäden im sechs- und siebenstelligen Euro Bereich.
    - Rückblickend auf das Jahr 2015 wissen wir von mehr als einem halben Duzend dieser Angriffe.
    - Dabei bedienen sich Angreifer der Methode eines so genannten „**Business E-Mail Compromises**".
    - Im Rahmen der Aufklärung und der Beratung vor Ort hat SBA-Research gemeinsam mit CERT.at Lessons Learned aus diesen Vorfällen abgeleitet.
    - Das Federal Bureau of Investigation (FBI) warnt vor dieser Bedrohung global und nennt konkrete Zahlen: 2013 gab es über 2.100 bekannte Opfer weltweit mit einem Schaden von insgesamt rd. 215 Millionen US-Dollar.

Cyber Angriffe sind eine reale Bedrohung für klassische Geschäftsmodelle

- Der zielgerichtete Angriff auf ein Handelssystem einer russischen Bank mit dem Corkow-Trojaner war ein Novum im Jahr 2015.
- Binnen 14 Minuten wurden durch die Angreifer Kauf- und Verkaufsanweisungen in Millionenhöhe getätigt.
- Nach einer Studie von Verizon öffnen 23% der MitarbeiterInnen Phishing E-Mails und 11% klicken auf Anhänge; Schadsoftware findet somit oft den Weg ins Unternehmen.
- Nach dem Symantec Internet Security Report 2015 richten sich ein Drittel aller Angriffe bereits gegen KMU.
- Jedes Unternehmen ist gut beraten, sich zeitgerecht mit dem Thema Cyber Sicherheit zu beschäftigen und eine für seine Größe und sein Geschäftsmodell ausgerichtete Cyber Sicherheits Strategie zu erstellen, um sich auf Angriffe vorzubereiten.

(C) Update: Österreichische Strategie für Cyber Sicherheit

- Mit der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) wurde von der Bundesregierung am 20. März 2013 ein umfassendes und proaktives Konzept zum Schutz des Cyber Raums und der Menschen in eben diesem beschlossen.
- Eine eigene Cyber Sicherheit Steuerungsgruppe unterstützt die Umsetzung der Strategie in Österreich entlang der folgenden sieben definierten Handlungsfelder:
    - Handlungsfeld 1: Strukturen und Prozesse
    - Handlungsfeld 2: Governance
    - Handlungsfeld 3: Kooperation Staat, Wirtschaft und Gesellschaft
    - Handlungsfeld 4: Schutz kritischer Infrastrukturen
    - Handlungsfeld 5: Sensibilisierung und Ausbildung
    - Handlungsfeld 6: Forschung und Entwicklung
    - Handlungsfeld 7: Internationale Zusammenarbeit

(D) Ausblick: Richtlinie für Netzwerk- und Informationssicherheit und Cyber Sicherheitsgesetz

- Am 7. Februar 2013 veröffentliche die EU- Kommission eine gemeinsame Mitteilung zur „Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum", sowie begleitend dazu den Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informations-sicherheit (NIS-RL) in der Union.
- Ziel der NIS-RL ist es, EU-weit eine hohe Sicherheit der Netzwerk- und Informationssysteme zu erreichen.
- Es soll die Zusammenarbeit der Mitgliedstaaten gestärkt sowie bestimmte Anbieter zu Sicherheitsmaßnahmen und Meldung gröberer Störfälle verpflichtet werden.
- Es ist mit einer Annahme der NIS-RL im Februar/März 2016 zu rechnen.
- Das österreichische Cyber Sicherheitsgesetz soll künftig die ÖSCS mit der NIS-RL zusammenführen.

(E) Ausblick: Cyber Sicherheits Trends und Gefahren von morgen

- McAfee rechnet bis 2020 mit mindestens 200 Milliarden vernetzten Geräten weltweit.
- Die Nachfrage nach Verarbeitung großer Datenmengen – Big Data – wird steigen.
- Die Cloud als Speicherform oder „Arbeitsplatz der Zukunft" etabliert sich nach und nach. Eine Erhebung von Eurostat (2014) ergab, dass 19% der Unternehmen in der EU Cloud Dienste nutzen. In Österreich nutzen sie nur 12%, während Unternehmen aus Finnland mit 51% die Spitzenreiter in Europa sind.
- Mobilität als Treiber von Flexibilisierung: Laut einer Gartner Umfrage verwenden 85% der befragten PrivatnutzerInnen der USA und 77% aus dem Rest der Welt mehrere Geräte gleichzeitig.
- Die Hacker Szene unterliegt einem kontinuierlichen Trend der Professionalisierung, der sich 2016 fortsetzen wird.
- Das aufkommende Social Engineering könnte auch in Zukunft eine wachsende Bedrohung darstellen. Dazu gehören Angriffsversuche via Telefon, Messaging, E-Mail und über Social Media.

- Durch das IoT, Cloud Dienste und Mobilität wird das Muster der Datenübertragung vor Herausforderungen gestellt. Gerade auch in Österreich mit den vielen ländlichen Regionen ist u.a. der Breitbandausbau Grundlage für wirtschaftliche Weiterentwicklung.

Weitere Informationen

- Download der **vollständigen Ausgabe** des „Berichts Internet-Sicherheit Österreich 2015“ auf der Website des Computer Emergency Response Teams (CERT.at): http://www.cert.at
- **Weitere Informationen** zum Thema auch auf den Webseiten von
  - Plattform Digitales Österreich: http://www.digitales.oesterreich.gv.at/
  - Computer Emergency Response Team für die öffentliche Verwaltung (GovCERT): http://www.govcert.gv.at

Rückfragehinweise

Büro Mag.[a] Sonja Steßl, Staatssekretärin für Digitales, Verwaltung und öffentlichen Dienst
Kontakt: Mag.a Petra Hafner, Pressesprecherin
Tel.: +43 1 531 15-204062
Mobil: +43 664 610 6384
Mail: petra.hafner@bka.gv.at

Pressestelle CERT.at
pantarhei corporate advisors
Kontakt: Mag. Markus Gruber
Mobil: +43 664 886 56 359
Mail: markus.gruber@pantarhei-advisors.com