Das 1x1 der IT-Sicherheit

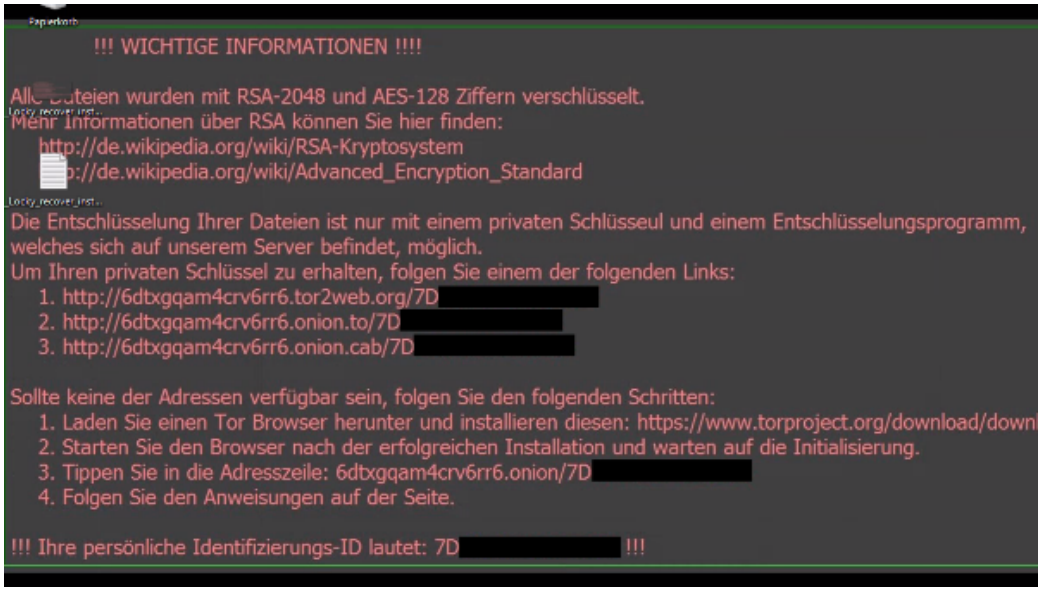
Cornelia Schildt, eco e.V.

Handwerkskammer Düsseldorf – 4.4.2017

WIR GESTALTEN DAS INTERNET.
GESTERN. HEUTE. ÜBER MORGEN.

eco
VERBAND DER INTERNETWIRTSCHAFT

Eines Morgens im Büro

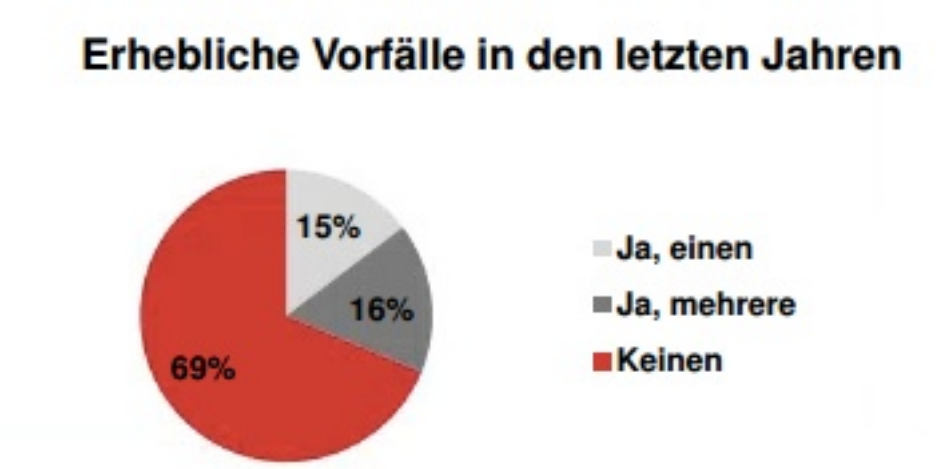


Quelle: https://upload.wikimedia.org/wikipedia/commons/1/17/Locky_trojan_02-2016_German_PD.png

3 Mythen der IT-Sicherheit

„Bei uns ist noch nie etwas passiert.“

3 Mythen der IT-Sicherheit



Erkennen Sie alle Vorfälle?

Quelle: eco Studie Internetsicherheit 2016

3 Mythen der IT-Sicherheit

„Angriffe treffen immer nur die Großen.“

Automatisierte Angriffe können jeden treffen

Erpressungstrojaner: Stadtverwaltung kauft sich mit 1,3 Bitcoin frei

heise online 04.03.2016 15:38 Uhr – Axel Kannenberg vorlesen

Eine Infektion mit dem Trojaner Teslacrypt legte im Februar die IT-Systeme der bayerischen Kleinstadt Dettelbach lahm. Die Verwaltung entschied sich das Lösegeld, zu zahlen - und kann nun zumindest teilweise wieder an ihre Daten.

12. Februar 2016, 16:36 Uhr Hackerangriff

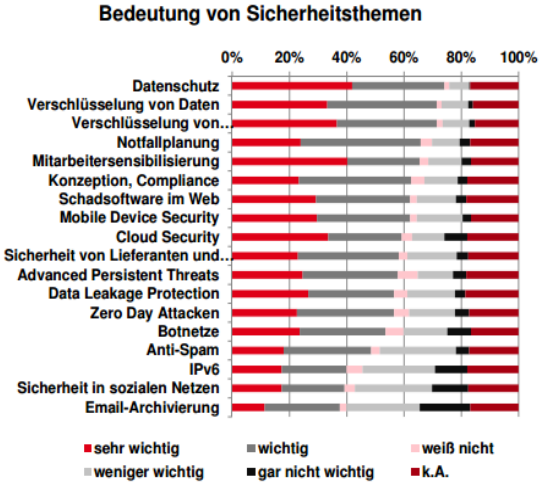
Computervirus legt Klinik in Neuss lahm

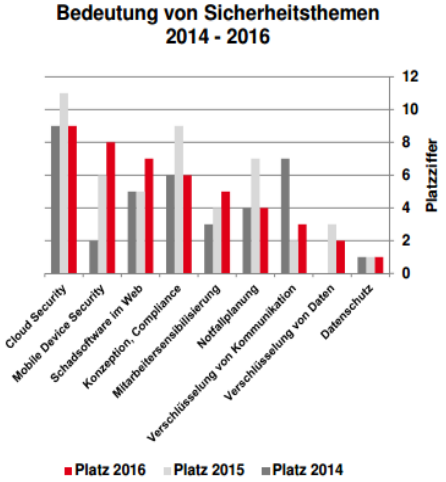
- Ein Computervirus legt das städtische Krankenhaus in Neuss lahm. Es werde gearbeitet wie vor 15 Jahren, sagt eine Sprecherin.
- Cyberangriffe auf Krankenhaus-IT nähmen zu, es gebe auch Fälle von Erpressung, teilt die Krankenhausgesellschaft mit.

3 Mythen der IT-Sicherheit

„Absolute Sicherheit gibt es nicht“

Bedeutung von Sicherheitsthemen





Sicherheitsmaßnahmen müssen angemessen sein

Quelle: eco Studie Internetsicherheit 2016

Aber

„Schon mit einfachen Mitteln kann das Schutzniveau angehoben werden“

Einfallstor Internetnutzung

Berthold - Lewis Leathers
An: decix
[SPAM] Rechnung Nr. V71795-785 Online Auktion Nr.71795 vom 07.03.2016 64

Sehr geehrte Damen und Herren,

als Anlage senden wir Ihnen die Rechnung (gilt als Original) für die von Ihnen ersteigerten Artikel bei der Online-Auktion Nr. 71795 vom 07.03.2016.

Wir bitten um Zahlungseingang bis zum 08.03.2016. Bitte geben Sie als Verwendungszweck die komplette Rechnungsnummer an.

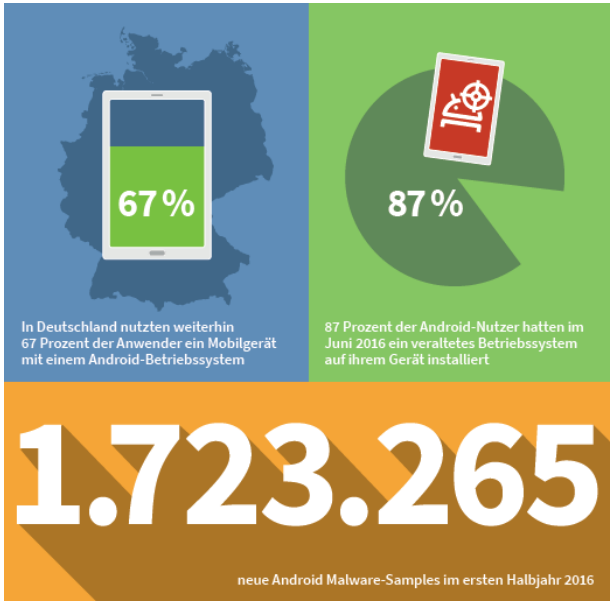
Freundliche Grüße Ihr Surplex Auction Team

Surplex GmbH Wahlerstr. 4 19406 Düsseldorf Germany Geschäftsführer: Michael Werker, Ulrich Stalter, Amtsgericht Düsseldorf, HRB 88779, USt-ID DE286740917

V71795-376_41179.doc

- Schadprogramme über E-Mail-Anhänge und verseuchte Webseiten
- Mit und ohne Zutun des Nutzers
- Hochprofessionelle Angreifer
- Opfer werden zu Tätern

Einfallstor Mobilgeräte



Quelle: G DATA Mobile Malware Report H1/2016

- Verändertes Nutzungsverhalten
- Stark gewachsener Funktionsumfang
- Alle 9 Sekunden ein neue Android–Schädling
- Durch „klassische“ Schutzmaßnahmen nicht abgedeckt

Einfallstor Mensch

Quelle: known_sense

- Social Engineering ergänzt technische Angriffe
- Ausnutzen von Hilfsbereitschaft, Neugier aber auch Angst
- Unzufriedene Mitarbeiter werden zum Innentäten

Exkurs CEO - Fraud

„CEO-Fraud"-Masche: Angestellte überweist mehrere zehntausend Euro

Autozulieferer Leoni um 40 Millionen Euro betrogen

Chef-Fraud oder Enkeltrick 4.0: Wie Betrüger Millionen ergaunern – und ihnen der Antwort-Button dabei hilft

AUFSICHTSRAT TAGTE

EVN wurde Ziel eines Betruges

- Mail des CEO an Buchhaltung hohen Geldbetrag ins Ausland zu überweisen
- Dringlichkeit & Vertraulichkeit

- Vorabrecherche mit öffentlichen Informationen oder Social Engineering

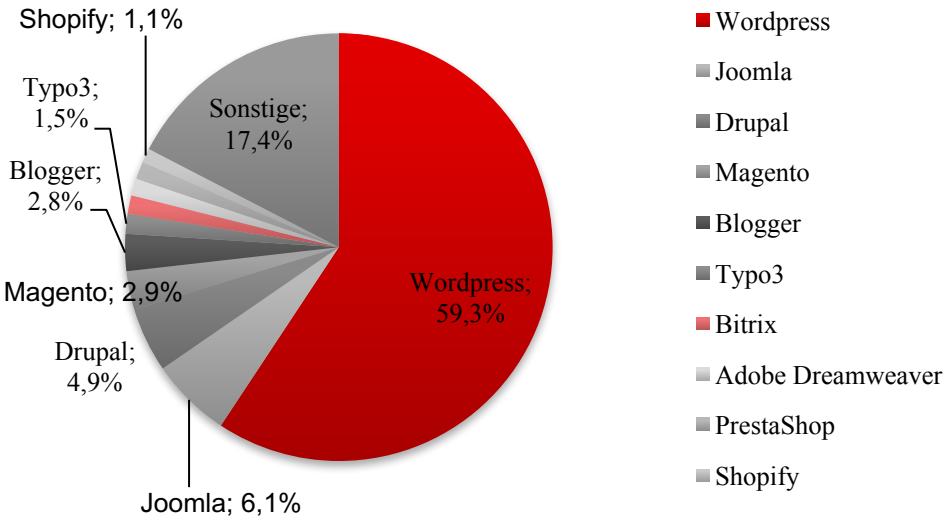
Einfallstor Webseite

97% der Angriffe auf Sicherheitslücken von weit verbreiteter Standardsoftware bei

- Web-Anwendungen
- Web-Servern
- Content Management-Systemen
- Plugins der CMS

Shellshock:
20 Jahre alter Fehler im Bash-Code. Betrifft alle Unix-Systeme seit 1994.
Poodle:
SSL – Fehler, wurde seit 1999 von Version zu Version weitervererbt.
Heartbleed:
Elementarer Grundfehler in der SSL-Verschlüsselung.

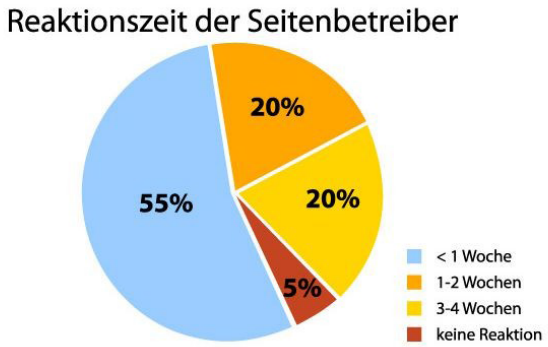
Einfallstor Webseite



Marktanteile CMS-Systeme (April 2016)

- Standard-CMS wie Wordpress, Joomla und Typo3 häufig eingesetzt
- Besonders erfolgreich wenn technische Betreuung der Webseiten zweitrangig ist und der Fokus rein auf den Inhalten liegt
- Angriffe können jeden Treffen – denn die meisten Angriffe sind nicht gezielt, sondern automatisiert

Einfallstor Webseite



- Großteil solcher Angriffe lässt sich mit einfachen Mitteln „vermeiden“
- Knapp die Hälfte aller Webseitenbetreiber ist nicht in der Lage, ein Update innerhalb einer Woche einzuspielen
- Die Reaktionszeiten von Webseitenbetreibern sind zu lang– auch nach einem Angriff

Was tun um ihre Sicherheit zu verbessern?

- Seien Sie sich der Gefahren bewußt!
- Betriebssystem, Anwendungsprogramme , Geräte und Webseiten aktuell halten
- Anti-Viren-Programme sind Pflicht (und nicht nur unter Windows)
- Im Falle eines Falles: Don‘t panic!

Wo bekomme ich Hilfe?

- Allgemeine Informationen
- www.bsi-fuer-buerger.de
- www.nrw-units.de

- Hilfe bei Schadprogrammen
- www.botfrei.de

- Hilfe für Webseiten
- www.initiative-s.de
- www.siwecos.de

Initiative-S hilft mit 3 Klicks

SIWECOS
Auf der sicheren Seite

Gefördert durch:

IT-Sicherheit
IN DER WIRTSCHAFT

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Partner und Unterstützer

cms garden

RUHR
UNIVERSITÄT
BOCHUM
RUB

HACKMANIT

SIWECOS hilft Webseitenbetreibern

- Projekt im Rahmen der Initiative "IT-Sicherheit in der Wirtschaft" des BMWi (Sep 2016 – Nov 2018)

Initiative „IT-Sicherheit in der Wirtschaft"
Die Initiative „IT-Sicherheit in der Wirtschaft" des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemein-sam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwal-tung soll eine Grundlage dafür geschaffen werden, um die Bewusstseins-bildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter: www.it-sicherheit-in-der-wirtschaft.de abrufbar.

SIWECOS hilft Webseitenbetreibern

Mehr erfahren unter
https://www.siwecos.de

SIWECOS steht für
Sichere Webseiten und Content Management Systeme und hilft Ihrem Betrieb Sicherheitsprobleme auf Ihrer Webseite rasch **zu erkennen und zu beheben**.

SIWECOS
Auf der sicheren Seite

SIWECOS hilft Webseitenbetreibern

- einen Webseitencheck, der Sicherheitslücken in Content Management Systemen aufdeckt.
- individuelle Benachrichtigungen und Handlungsempfehlungen zu Sicherheitsproblemen auf Ihrer Webseite.
- kompetente Ansprechpartner mit jahrelanger Erfahrung im Bereich IT-Sicherheit.
- und das alles völlig kostenlos

Mehr erfahren unter
https://www.siwecos.de

www.eco.de
www.botfrei.de
www.initiative-s.de
www.siwecos.de

Kontakt

Cornelia Schildt
eco – Verband der Internetwirtschaft e.V.
www.eco.de

Lichtstraße 43h
50825 Köln

Fon +49 (0) 221 – 7000 48-175
Fax +49 (0) 221 – 7000 48-111

cornelia.schildt@eco.de