Workshop 3:
Viren-Terror im Zeitalter von E-Health:

Chancen und Gefahren der Digitalisierung im Praxis-Alltag

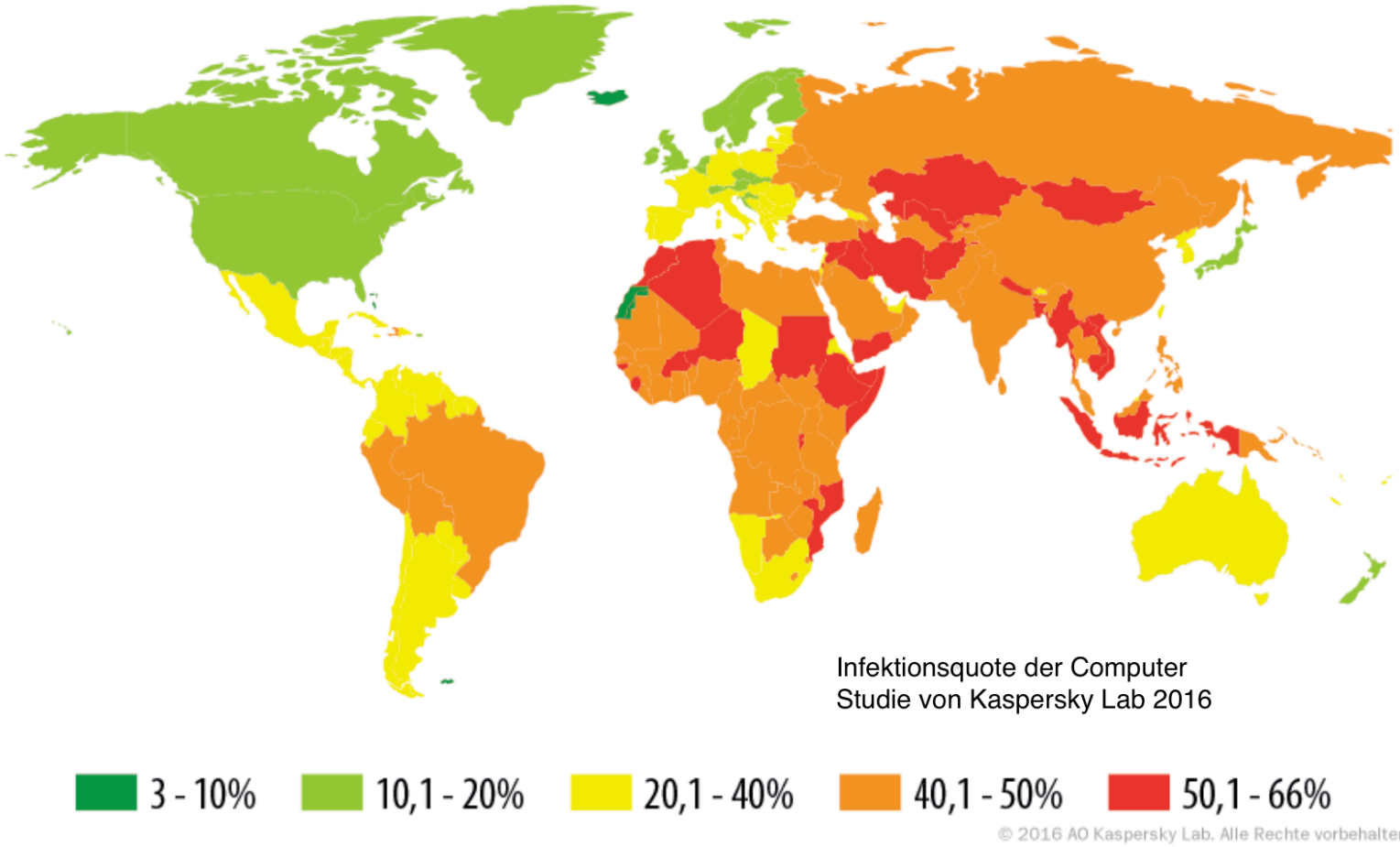
TEAMWORK IN DER ARZTPRAXIS

Unternehmertagung für niedergelassene Ärztinnen und Ärzte und ihr Praxisteam

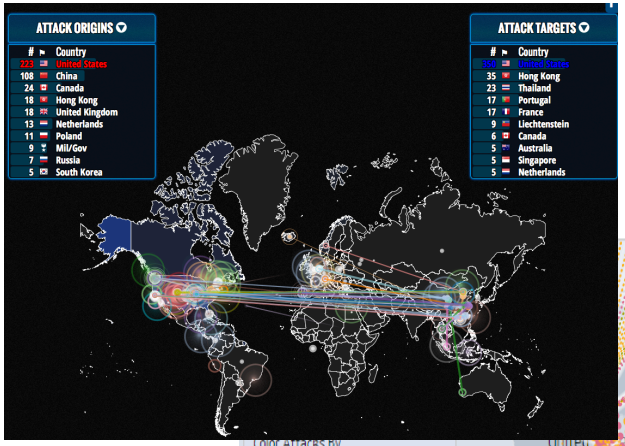
Agenda

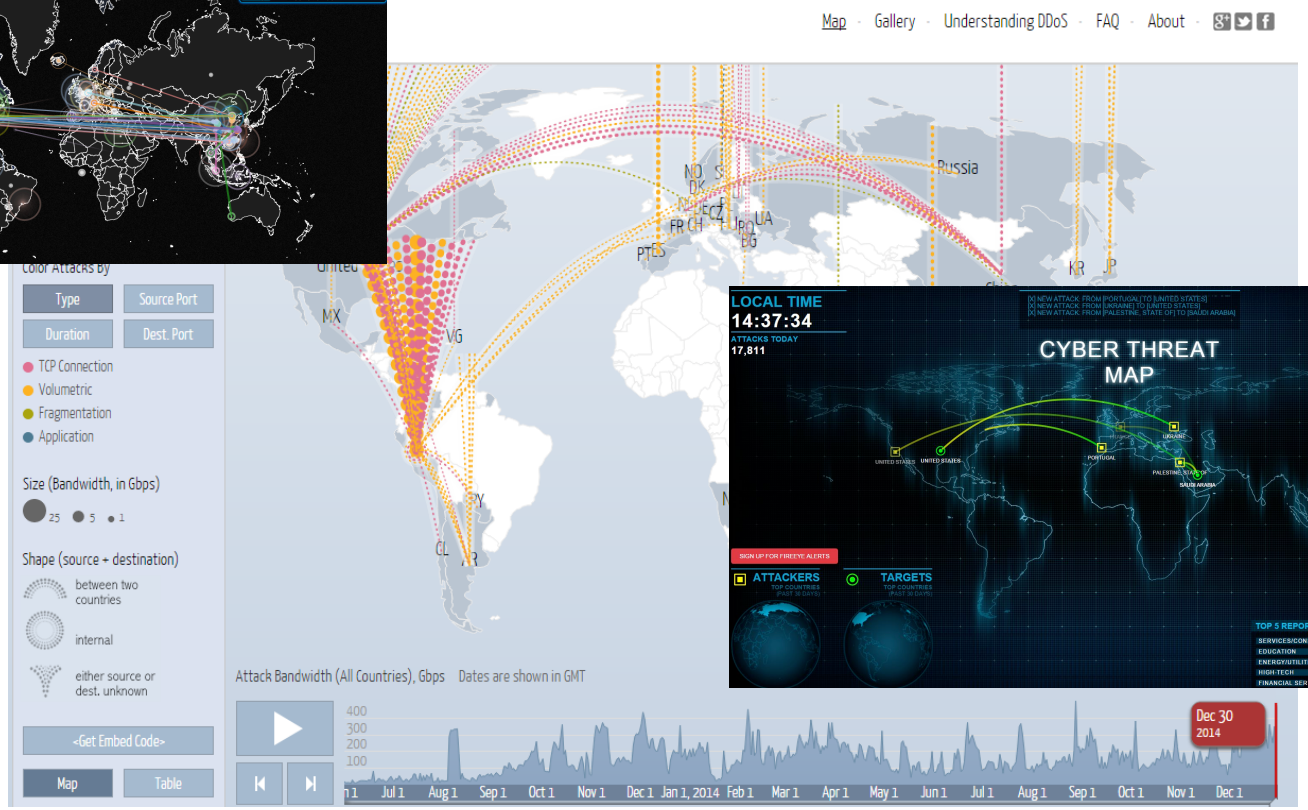
- Cyber-Attacken – Wie schlimm ist es wirklich?
  - Infizierte Computer, Cyber Attack Maps und was sagen die Ärzte
- Google Hacking
- Internet of things und SHODAN
- Maleware und Trojaner
- Social Engineering
- Gegenmassnahmen

Cyber-Attacken – Wie schlimm ist es wirklich?
- Mit Schadsoftware infizierte Computer – Status 2016



Cyber-Attacken – Wie schlimm ist es wirklich?
-Cyber Attack Maps





Cyber-Attacken – Wie schlimm ist es wirklich?

Hacker legen Spital lahm und verlangen Lösegeld

Cyber-Kriminelle halten in Los Angeles Patientendaten einer Klinik unter Verschluss. Sie fordern rund 3,7 Millionen Franken für die Freigabe.

Neue Schadsoftware Petya wird mittels Bewerbungsschreiben an Personal-Abteilungen verschickt

E-Mails gelten als bevorzugtes Mittel,um Schadsoftware zu verbreiten. Der Empfä
dazu verleitet werden, einen Link oder Anhang zu öffnen, mit dem Ziel, dass sich
Schadsoftware auf dem Computer installieren kann. Aktuell versucht sich die Sch
Petya mit einem fiesen Trick mittels Bewerbungsschreiben per E-Mail an Persona
Abteilungen von Unternehmen zu verbreiten. Es ist Vorsicht geboten, denn…

Tages-Anzeiger

Die unabhängige Schweizer Tageszeitung

Samstag
28. Mai 2016

Wochenende
Franz Steinegger und Peter Bodenmann diskutieren am Gotthard über die politische Angststarre in der Schweiz.

Furchtlo
Ein Chef
Kleider h
sehr Beru

Walliser Patientendossier bereits wieder offline

Nach massiver Kritik des Datenschutzbeauftragten und der Piratenpartei hat die Walliser Gesundheitsministerin Esther Waeber-Kalbermatten die Einführung der eHealt-Plattform «Infomed» verschoben.

– Von Patrick Bizzarri , 01.09.2015 13:55.

Letzte Woche wurde im Kanton Wallis das elektronische Patientendossier «Infomed» vorgestellt. Neben den Pionieren im Kanton

WEITERE ARTIKEL

- Kanton Wallis lanciert

Hacker dringen in Schweizer Arztpraxen ein

Die Cyber-Kriminellen verschlüsselten Patientendaten und wollten Geld erpressen.

Der FCZ-Chef will sich helfen lassen

Suizid eine

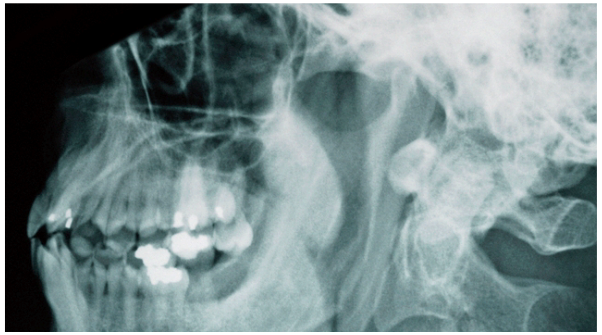
Tragische Entwicklung im Fall «Schumacher»

In der Nacht nach seiner Verhaftung ist ein Mann tot in seiner Zelle im Zürcher Polizeigefängnis gefunden worden. Der Rega-Mitarbeiter soll die Krankenakte von Michael Schumacher gestohlen haben.

von Marcel Gyr | 6.8.2014, 21:21 Uhr | 12 Kommentare

Patientendaten sind leichte Beute

Ein Test zeigt: Die IT-Netzwerke von Arztpraxen weisen zum Teil gravierende Sicherheitslücken auf. Das kann auch für Patienten gefährlich werden.



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.

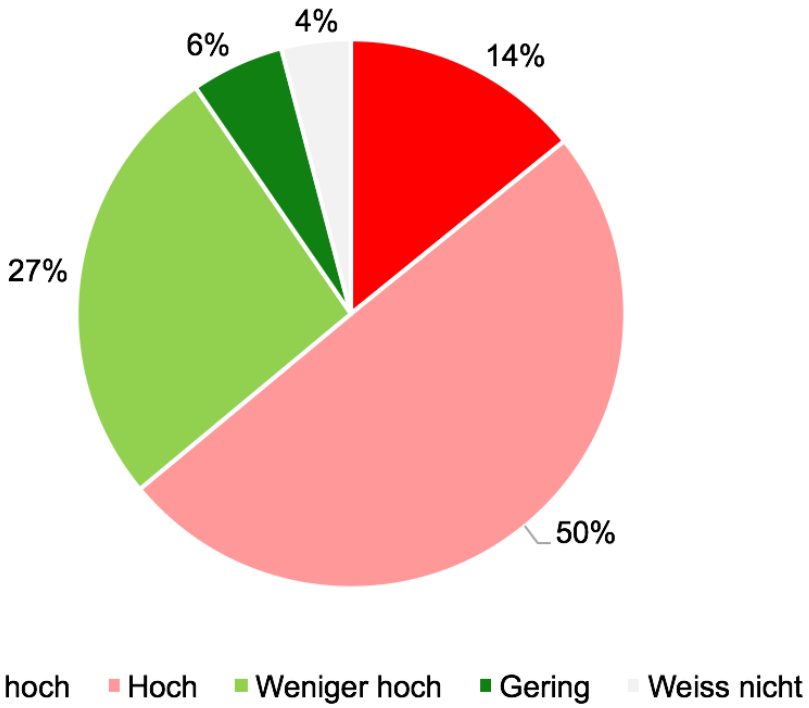
Digitalisierung und Schadprogramme

- Bedrohung durch Schadprogramme
- Einschränkung durch die Bedrohung
- Massnahmen nach Praxisart
- Aufwand nach Praxisart

Ärztebarometer
Zentrale Resultate
1. April 2017
Seite 4

Bedrohung durch Schadprogramm

Wie hoch schätzen Sie allgemein die Bedrohung durch Schadprogramme für Arztpraxen ein?

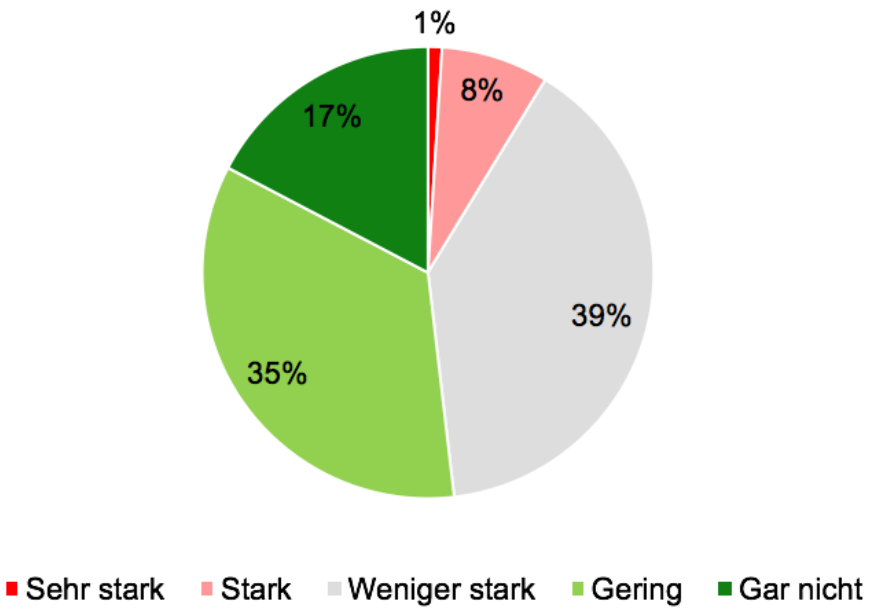


KMU-HSG

Ärztebarometer
Zentrale Resultate
1. April 2017
Seite 32

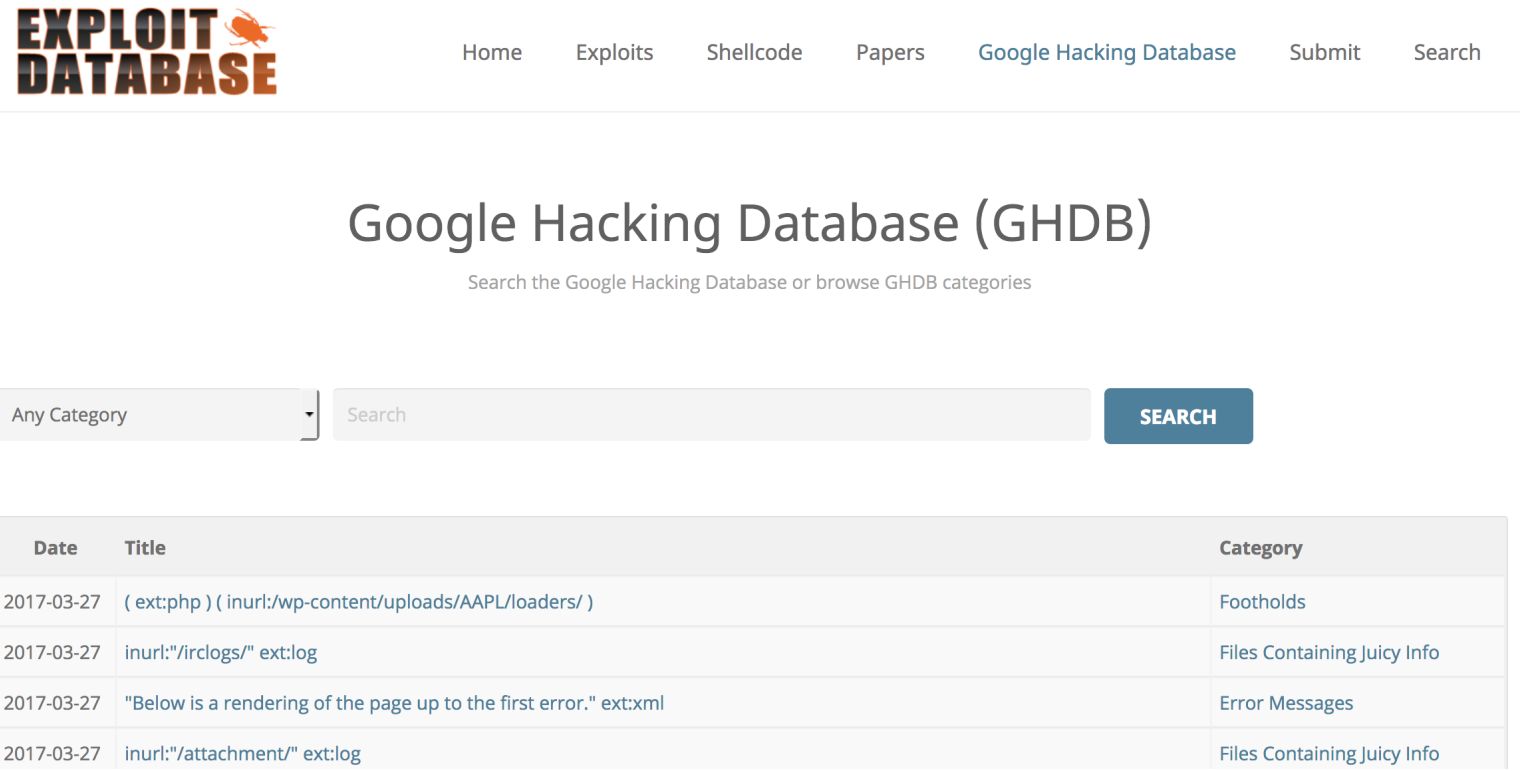
Einschränkung durch Bedrohung

Wie stark schränkt Sie die Bedrohung durch Schadprogramme in Ihrer eigenen Arbeit ein?



KMU-HSG

Google Hacking



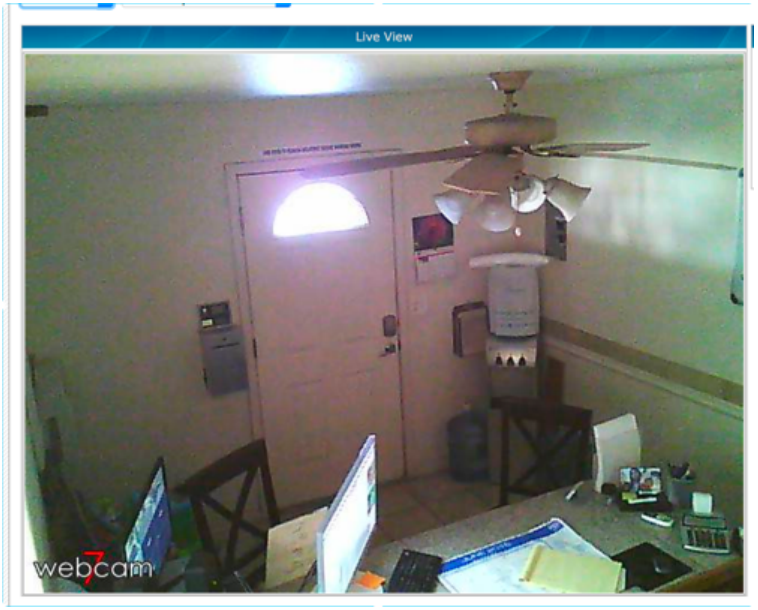
Internet of things and SHODAN:
Viele ans Internet angeschlossene Geräte sind ungeschützt

Web-Kameras

- **Überwachungskameras**
- **Private Webcams**

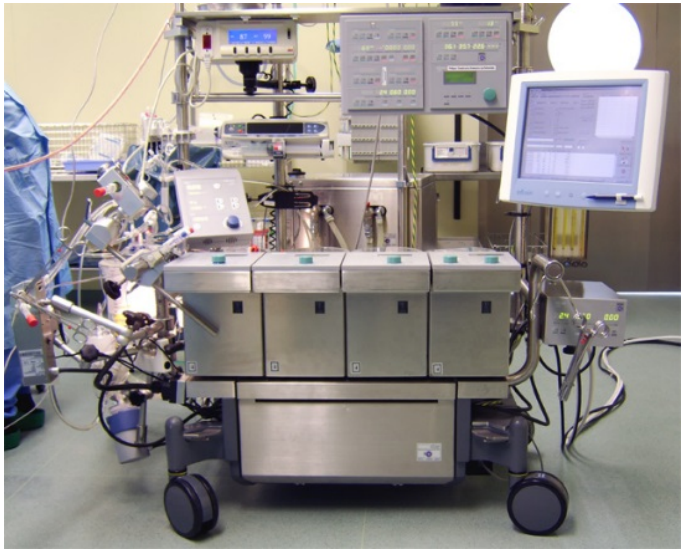
Steuerungsgeräte

- **Industrieanlagen**
- **Telefonanlagen/Konferenzen**



Internet of things gibt es auch im medizinischen Umfeld…

Herz-Lungenmaschine mit
Web-Zugang für die Wartung

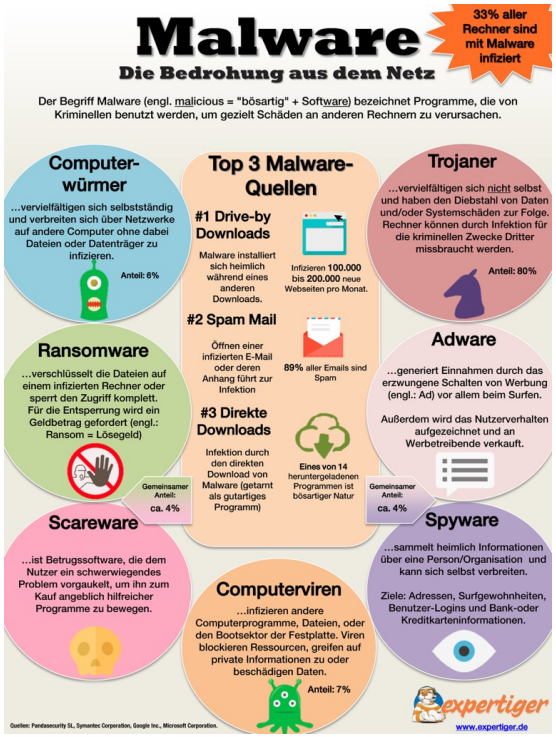


Infusionspumpe mit Internetzugang
für Konfiguration durch Hersteller

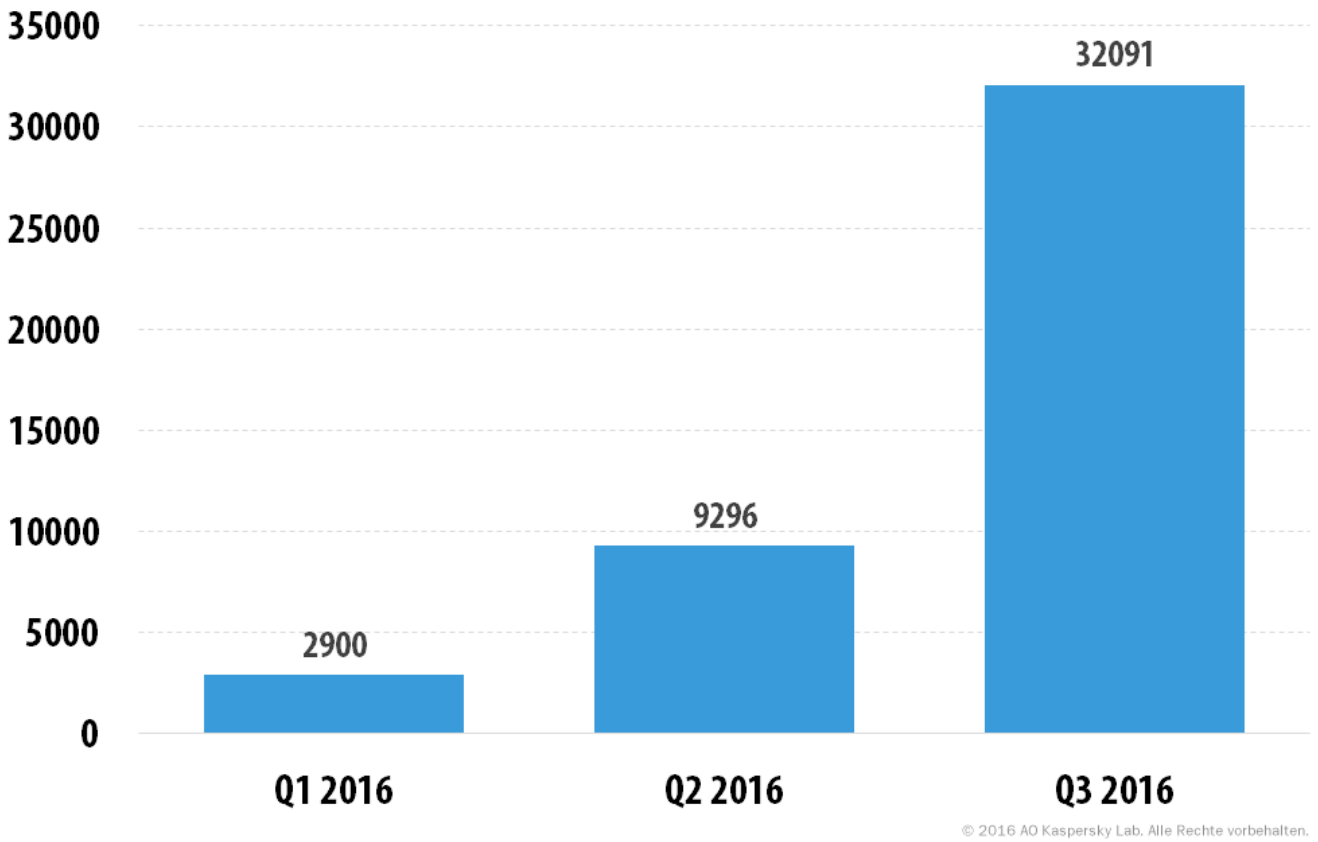
Malware, Viren und Trojaner gehören alle zur Gattung Schadsoftware

Als Schadsoftware (Malware) bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen auszuführen.

Ist ein Computer von Schadsoftware befallen, kann es sein, dass Daten nicht mehr vor unberechtigten Zugriffen geschützt sind und der Computer ferngesteuert werden kann.

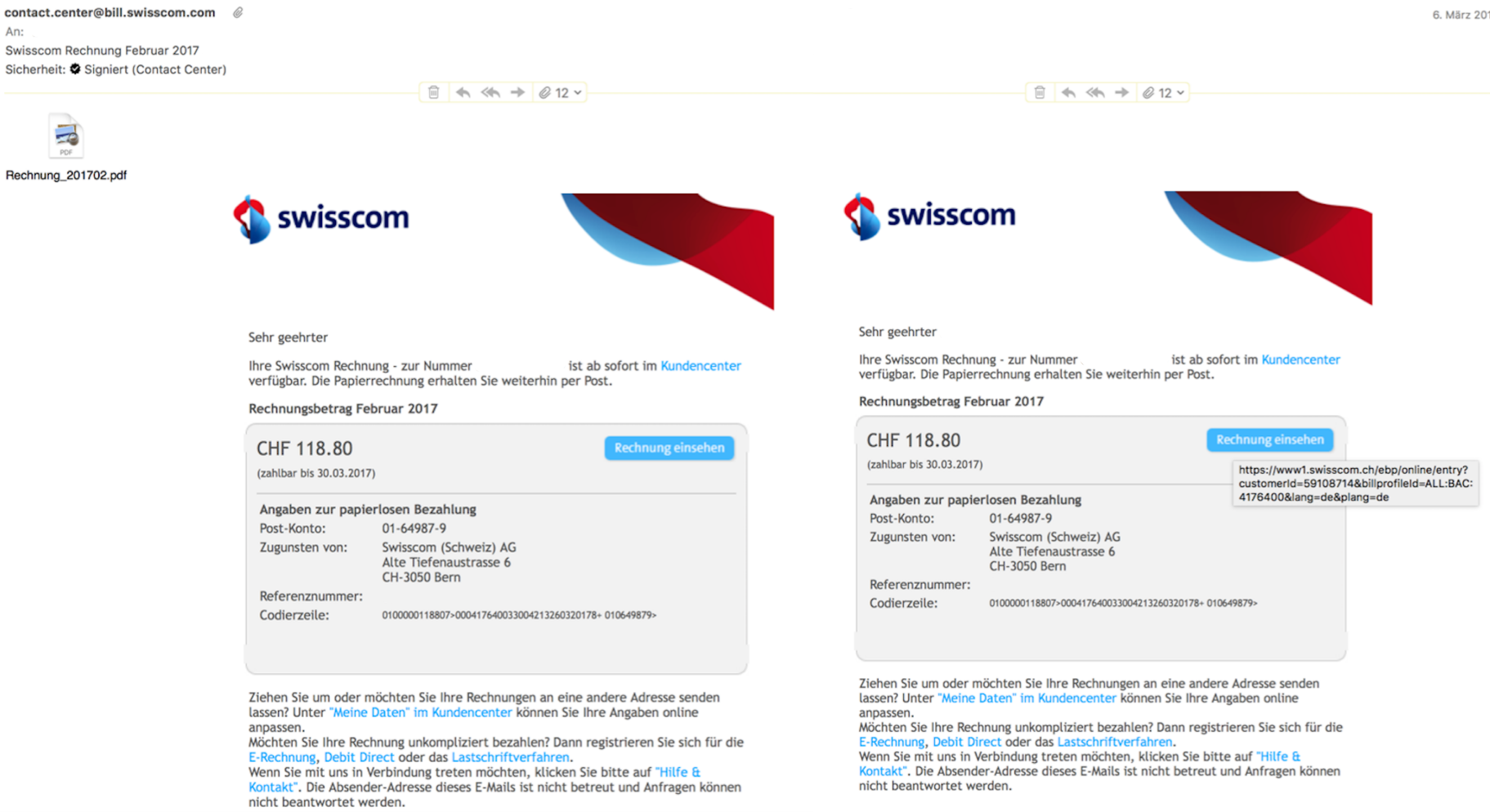


Beispiel Verschlüsselungstrojaner: Die Malware-Industrie entwickelt laufend und zu tausenden neue Modifikationen



Zahl neuer Modifikationen von Verschlüsselungstrojanern, erstes Quartal bis drittes Quartal 2016

Maleware und Trojaner:
Alle Schutzmassnahmen sind nur so stark wie das schwächste Glied in der Kette



contact.center@bill.swisscom.com
An:
Swisscom Rechnung Februar 2017
Sicherheit: Signiert (Contact Center)

6. März 2017

Rechnung_201702.pdf

swisscom

Sehr geehrter

Ihre Swisscom Rechnung - zur Nummer ist ab sofort im Kundencenter verfügbar. Die Papierrechnung erhalten Sie weiterhin per Post.

Rechnungsbetrag Februar 2017

CHF 118.80
(zahlbar bis 30.03.2017)
Rechnung einsehen

Angaben zur papierlosen Bezahlung

Post-Konto:	01-64987-9
Zugunsten von:	Swisscom (Schweiz) AG Alte Tiefenaustrasse 6 CH-3050 Bern
Referenznummer:	
Codierzeile:	0100000118807>000417640033004213260320178+ 010649879>

Ziehen Sie um oder möchten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter können Sie Ihre Angaben online anpassen.
Möchten Sie Ihre Rechnung unkompliziert bezahlen? Dann registrieren Sie sich für die E-Rechnung, Debit Direct oder das Lastschriftverfahren.
Wenn Sie mit uns in Verbindung treten möchten, klicken Sie bitte auf "Hilfe & Kontakt". Die Absender-Adresse dieses E-Mails ist nicht betreut und Anfragen können nicht beantwortet werden.

swisscom

Sehr geehrter

Ihre Swisscom Rechnung - zur Nummer ist ab sofort im Kundencenter verfügbar. Die Papierrechnung erhalten Sie weiterhin per Post.

Rechnungsbetrag Februar 2017

CHF 118.80
(zahlbar bis 30.03.2017)
Rechnung einsehen

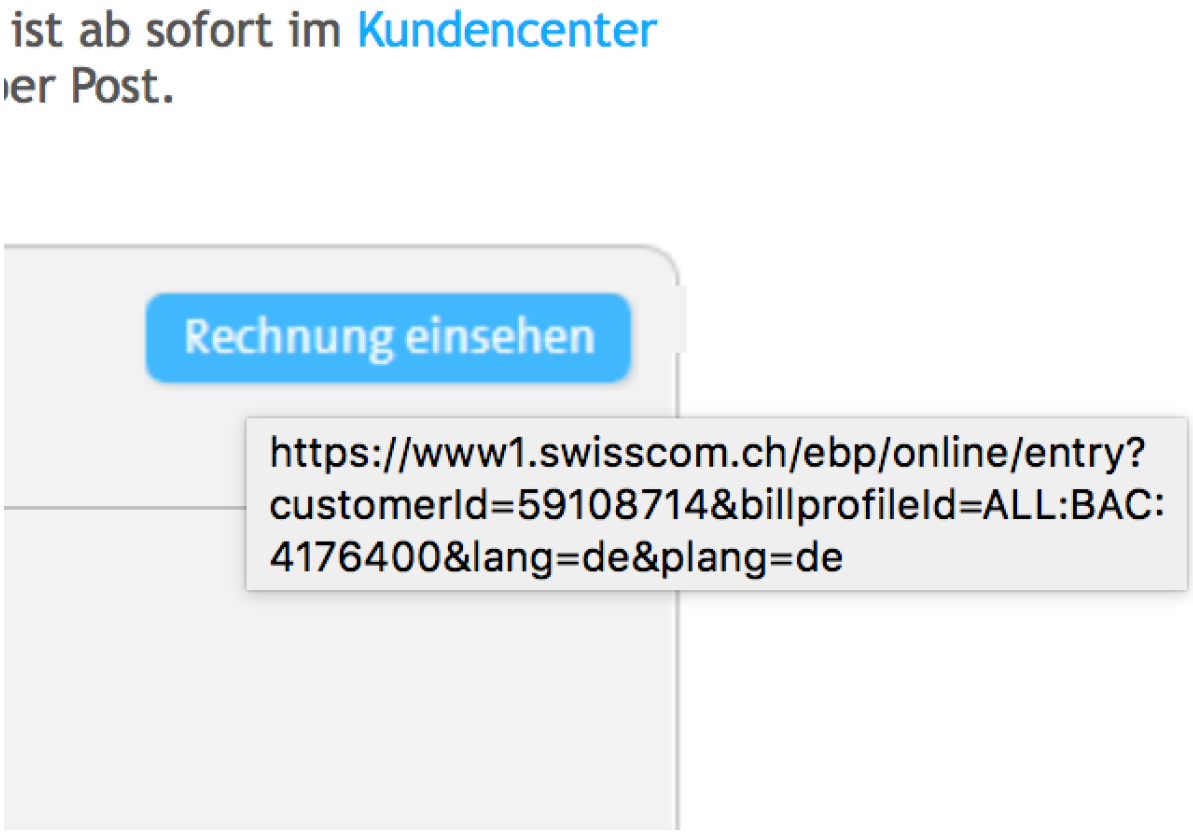
https://www1.swisscom.ch/ebp/online/entry?customerId=59108714&billprofileId=ALL:BAC:4176400&lang=de&plang=de

Angaben zur papierlosen Bezahlung

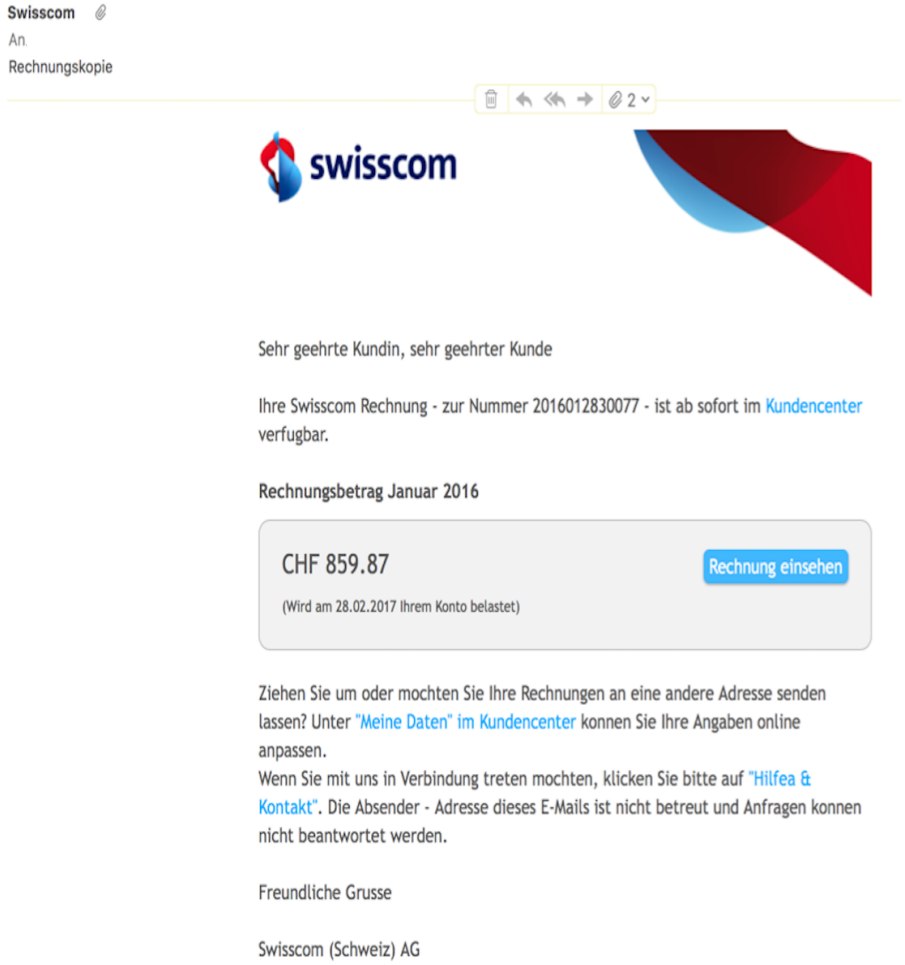
Post-Konto:	01-64987-9
Zugunsten von:	Swisscom (Schweiz) AG Alte Tiefenaustrasse 6 CH-3050 Bern
Referenznummer:	
Codierzeile:	0100000118807>000417640033004213260320178+ 010649879>

Ziehen Sie um oder möchten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter können Sie Ihre Angaben online anpassen.
Möchten Sie Ihre Rechnung unkompliziert bezahlen? Dann registrieren Sie sich für die E-Rechnung, Debit Direct oder das Lastschriftverfahren.
Wenn Sie mit uns in Verbindung treten möchten, klicken Sie bitte auf "Hilfe & Kontakt". Die Absender-Adresse dieses E-Mails ist nicht betreut und Anfragen können nicht beantwortet werden.

Maleware und Trojaner:
Alle Schutzmassnahmen sind nur so stark wie das schwächste Glied in der Kette



Maleware und Trojaner:
Alle Schutzmassnahmen sind nur so stark wie das schwächste Glied in der Kette



Swisscom
An
Rechnungskopie

swisscom

Sehr geehrte Kundin, sehr geehrter Kunde

Ihre Swisscom Rechnung - zur Nummer 2016012830077 - ist ab sofort im Kundencenter verfugbar.

Rechnungsbetrag Januar 2016

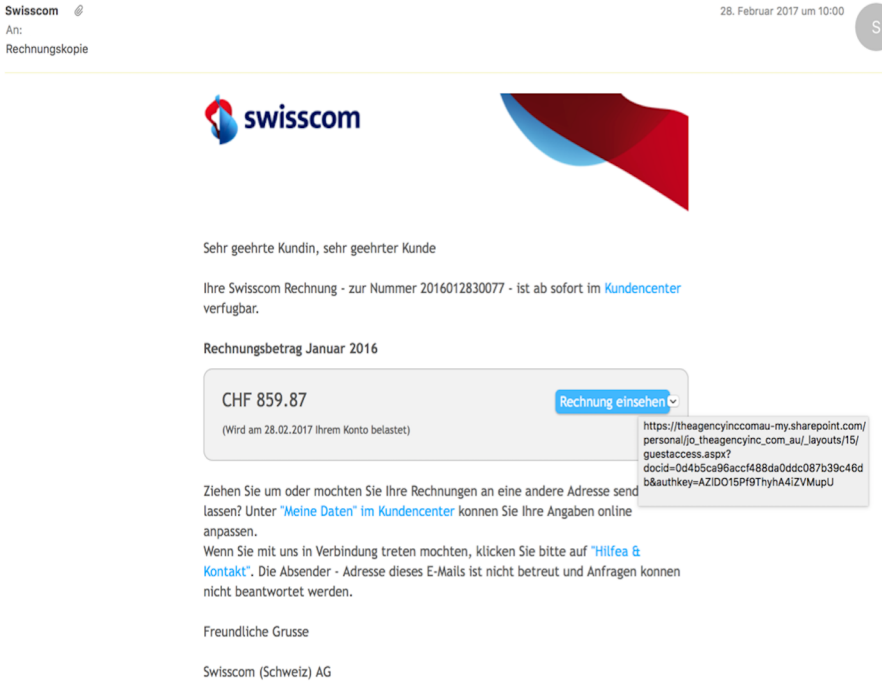
CHF 859.87 — Rechnung einsehen

(Wird am 28.02.2017 Ihrem Konto belastet)

Ziehen Sie um oder mochten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter konnen Sie Ihre Angaben online anpassen.
Wenn Sie mit uns in Verbindung treten mochten, klicken Sie bitte auf "Hilfea & Kontakt". Die Absender - Adresse dieses E-Mails ist nicht betreut und Anfragen konnen nicht beantwortet werden.

Freundliche Grusse

Swisscom (Schweiz) AG



Swisscom
An:
Rechnungskopie
28. Februar 2017 um 10:00

swisscom

Sehr geehrte Kundin, sehr geehrter Kunde

Ihre Swisscom Rechnung - zur Nummer 2016012830077 - ist ab sofort im Kundencenter verfugbar.

Rechnungsbetrag Januar 2016

CHF 859.87 — Rechnung einsehen

(Wird am 28.02.2017 Ihrem Konto belastet)

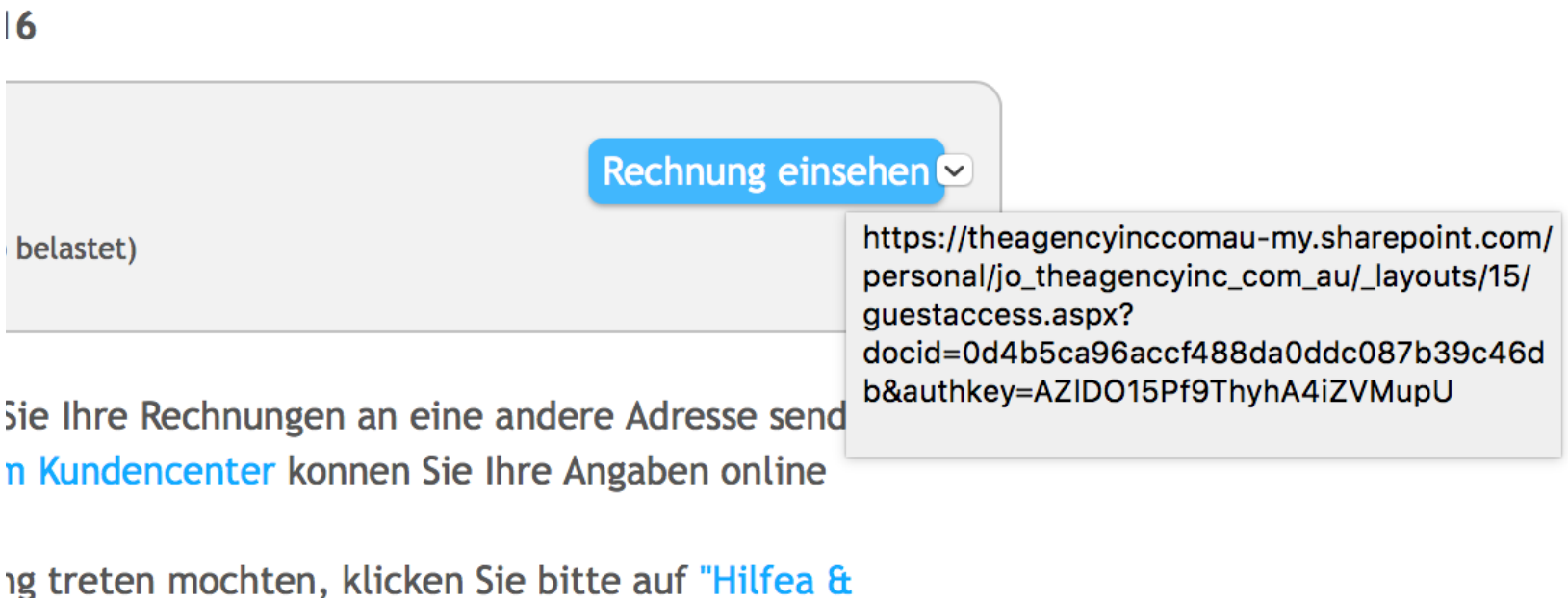
https://theagencyinccomau-my.sharepoint.com/personal/jo_theagencyinc_com_au/_layouts/15/guestaccess.aspx?docid=0d4b5ca96accf488da0ddc087b39c46db&authkey=AZlDO15Pf9ThyhA4iZVMupU

Ziehen Sie um oder mochten Sie Ihre Rechnungen an eine andere Adresse send lassen? Unter "Meine Daten" im Kundencenter konnen Sie Ihre Angaben online anpassen.
Wenn Sie mit uns in Verbindung treten mochten, klicken Sie bitte auf "Hilfea & Kontakt". Die Absender - Adresse dieses E-Mails ist nicht betreut und Anfragen konnen nicht beantwortet werden.

Freundliche Grusse

Swisscom (Schweiz) AG

Maleware und Trojaner:
Alle Schutzmassnahmen sind nur so stark wie das schwächste Glied in der Kette



Social-Engineering-Angriffe: Ausnutzen der Hilfsbereitschaft, Neugier und Gutgläubigkeit von Personen

Die IT-Sicherheit in einem Unternehmen ist nur so gut wie das schwächste Glied. Und das ist der Mensch. Viele der heutigen Angriffe erfolgen mit Social Engineering. Dabei versucht der Angreifer mittels Information Gathering an Informationen über die Firma oder die Mitarbeiter der Firma zu kommen, um diese dann für einen Angriff auszunutzen.

Social-Engineering-Angriffe: Ausnutzen der Hilfsbereitschaft, Neugier und Gutgläubigkeit von Personen

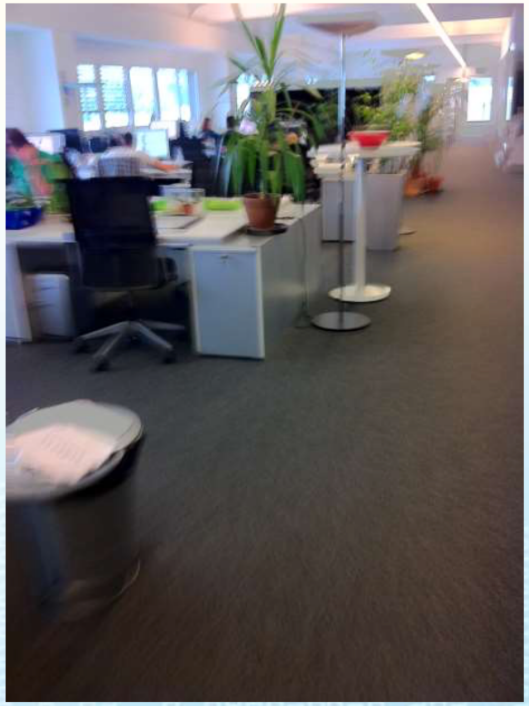
Ein Beispiel:

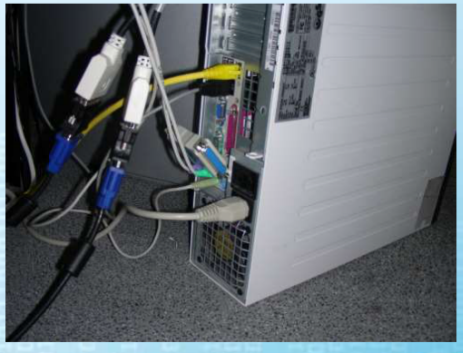
- Kontrolle des Arbeitsplatzes, «Dongle»

Strahlung- Messtechnik AG

Andreas Wisler
a.wisler@strahlung-messtechnik.ch

Militärstrasse 90
8004 Zürich
0041 44 240 10 10
info@strahlung-messtechnik.ch





Social Engineering – Drei Arten

•**Computer Based (technisch)**
Die Angriffe erfolgen mit technischen Mitteln. Unter anderem über E-Mails oder manipulierte Internetseiten mit Eingabefeldern. Ein Beispiel für diese Art ist das klassische Phishing.

•**Human Based (persönlich)**
Beim Human Based Social Engineering wird der Angriff persönlich über soziale Annäherung ausgeübt. Als Beispiel gibt sich der Angreifer als eine Autoritätsperson oder als Servicetechniker aus.

•**Reverse Social Engineering**
Eine weitere Ausprägung des Social Engineering ist das Reverse Social Engineering. Ziel des Angreifers ist es hier, das Opfer dazu zu bringen, sich beim Angreifer freiwillig zu melden. Dabei erfindet der Angreifer ein Problem und bittet zum Beispiel das Opfer um Hilfe, um es zu beseitigen. Das erhöht beim Opfer die Glaubwürdigkeit.

Google Hacks, Internet of things, Trojaner und Maleware, Social Engineering....

Was kann man tun?

Google Hacking - Gegenmassnahme

- Prüfen Sie regelmässig Ihre eigenen öffentlich erreichbaren Systeme
- Konfigurieren Sie Ihren Webserver richtig und achten Sie auf Sicherheitseinstellungen (robots.txt)
- Deaktivieren Sie Fehlermeldungen und Warnungen auf Ihren Webseiten
- Implementieren Sie ein Rechtekonzept und wenden Sie dieses auf all Ihren Webserver-Verzeichnissen an
- Überprüfen Sie Ihre Infrastruktur mit einem Schwachstellen-Scanner

Internet of things - Gegenmassnahme

Wenn Sie Komponenten kaufen die an Ihr Netz angeschlossen werden, achten Sie auf folgende Punkte:

- Erkundigen Sie sich im Vorfeld bei einem Spezialisten wie es bezüglich Sicherheit aussieht. Lassen Sie sich beraten
- Vergeben Sie immer ein sicheres Passwort
- Stellen Sie sicher, dass Standard-Passwörter deaktiviert sind
- Googlen Sie die Komponenten, die Sie kaufen wollen
- Überprüfen Sie Ihre Infrastruktur mit einem Schwachstellenscanner

Social Engineering - Gegenmassnahmen

Wie schütze ich mich?

Empfehlung MELANI

- Die Grundregel, bei zweifelhaften oder ungewöhnlichen Kontaktaufnahmen keine internen Informationen preiszugeben und keinen Aufforderungen nachzukommen, ist angesichts der derzeitigen Fälle aktueller denn je.
- Bei ungewöhnlichen Kontaktaufnahmen und Aufforderungen ist es empfehlenswert innerhalb der Firma telefonisch Rücksprache zu nehmen um die Richtigkeit des Auftrages zu verifizieren.
- Sämtliche Prozesse, welche den Zahlungsverkehr betreffen, sollten firmenintern klar geregelt sein und von den Mitarbeitenden in allen Fällen eingehalten werden.
- Insbesondere empfiehlt MELANI eine Sensibilisierung der Mitarbeitenden bezüglich dieser Vorfälle, insbesondere der Mitarbeitenden in Schlüsselpositionen.
- Opfer haben die Möglichkeit, speziell im Falle eines erfolgreichen Betruges, eine Strafanzeige bei der örtlich zuständigen Kantonspolizei zu erstatten.

Awareness zuerst