



Herausforderungen und Massnahmen aus Sicht eines grossen Providers

Informationssicherheit im Gesundheitswesen

23. Juni 2015

Christian Greuter, CEO Health Info Net AG



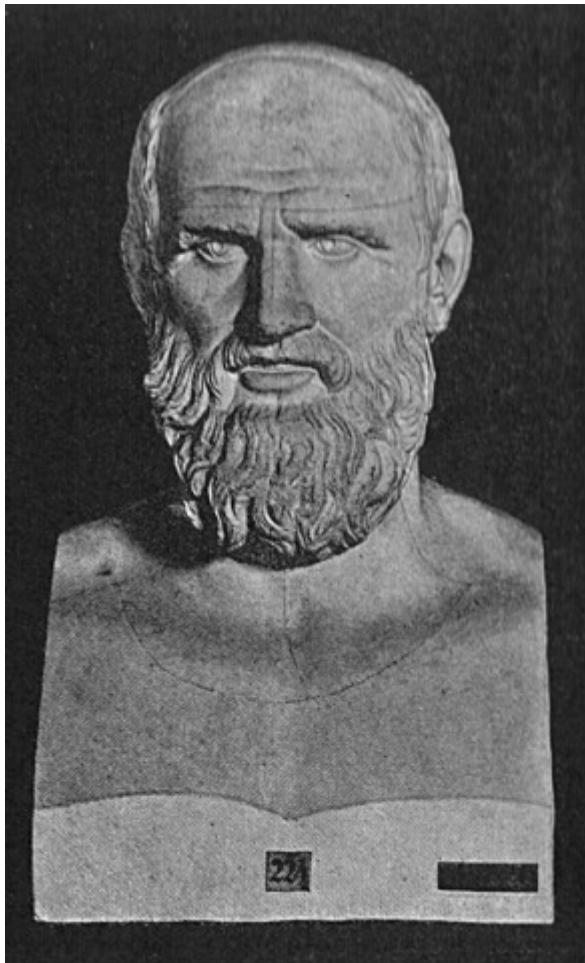
Agenda



- Einführung und Vorstellung HIN
- Trends als Herausforderung
- Grenzen der Machbarkeit
- Ausweg und Ausblick



Informationssicherheit im Gesundheitswesen ist ein uraltes Thema



Ἄ δ' ἂν ἐν θεραπείῃ ἢ ἴδω, ἢ ἀκούσω, ἢ καὶ ἄνευ θεραπήϊς κατὰ βίον ἀνθρώπων, ἃ μὴ χρή ποτε ἐκλαλέεσθαι ἔξω, σιγήσομαι, ἄρρητα ἡγεύμενος εἶναι τὰ τοιαῦτα.

Was ich bei der Behandlung oder auch ausserhalb meiner Praxis im Umgange mit Menschen sehe und höre, das man nicht weiterreden darf, werde ich verschweigen und als Geheimnis bewahren.



Die zweier Beziehung Arzt-Patient haben wir im Gesundheitswesen längst verlassen

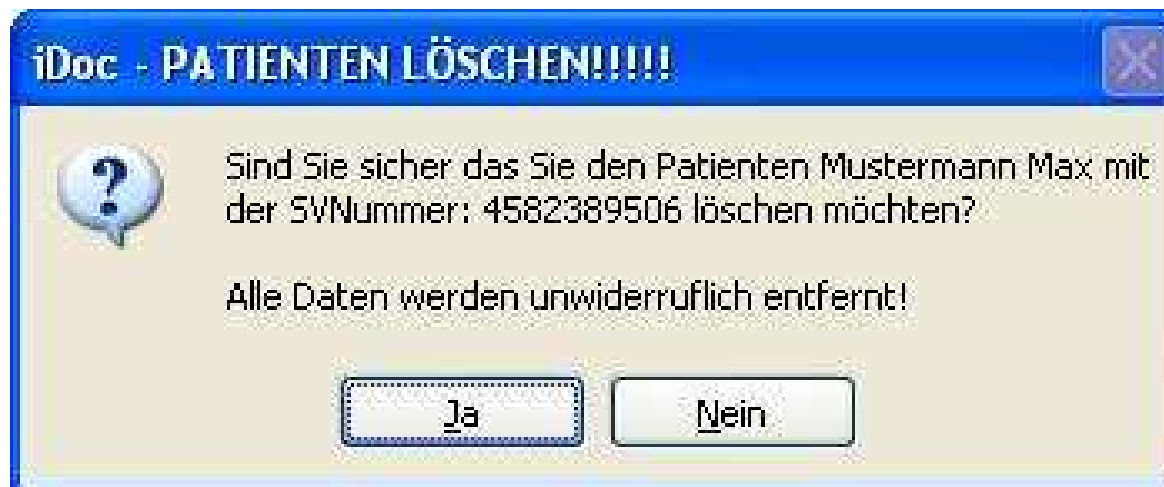




Themenspektrum ist gross, Fokus häufig der Schutz vor Einsicht und Verlust

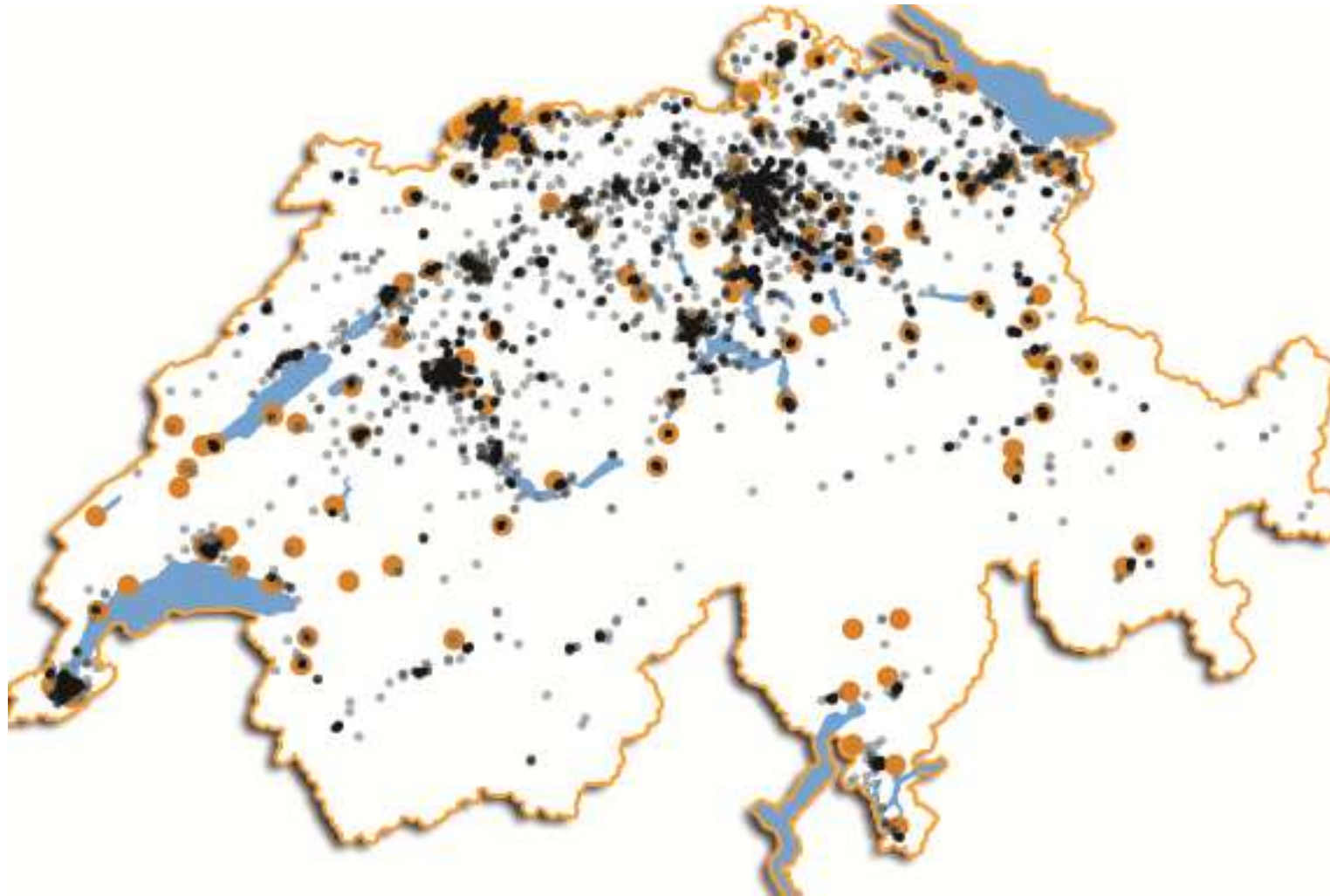


Als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, die die Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen.



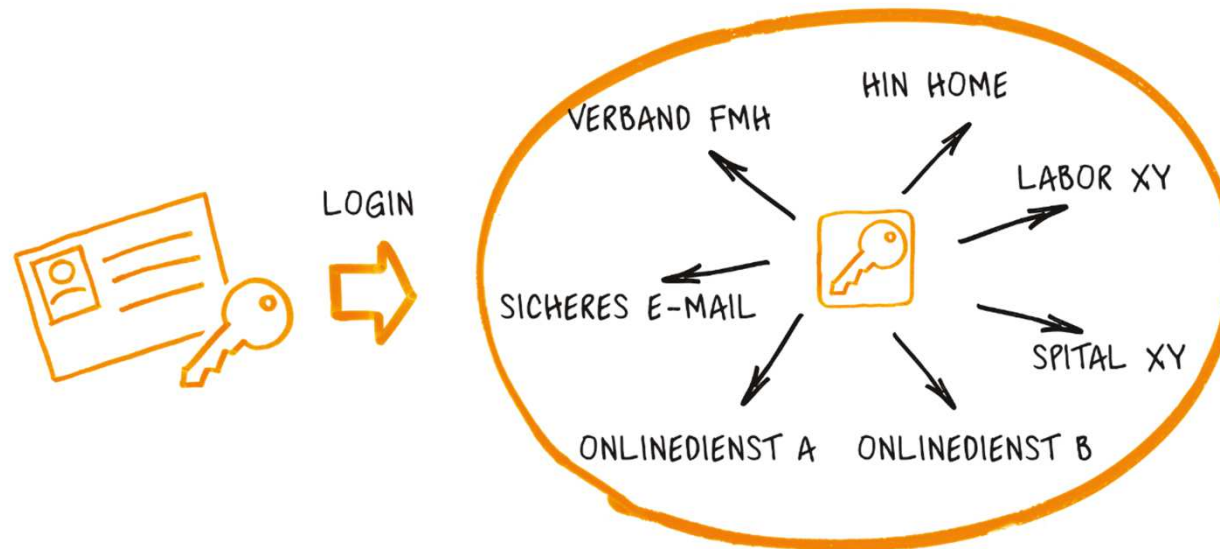


Aus der sicheren E-Mail entwickelte sich die Community mit über 17'000 Identitäten und 420 Institutionen





Kern aller Services ist die digitale Identität, welche HIN für Personen und Institutionen bereitstellt



Sichere Kommunikation
Datenschutzkonforme E-Mails



Sicherer Zugriff
Ein Benutzerprofil für elektronische Dienste



Sichere Zusammenarbeit
Kollaboration mit online Werkzeugen



Manchmal werden wir auch verwechselt...



Von: Health Info Net (HIN) [<mailto:dbowen747@aol.com>]

Gesendet: Mittwoch, 18. Juni 2014 11:38

An: undisclosed-recipients:

Betreff: E-Mail-Bestätigung



Sehr geehrter Kunde Health Info Net

Unsere Aufzeichnungen zeigen, dass Ihr Konto wurde nicht aktualisiert als Teil unserer normalen Kontoführung. unseren neuen SSL Server überprüfen jedes Konto für die Tätigkeit Ihrer Information hat nach dem Zufallsprinzip für die Prüfung ausgewählt Health Info Net Center unserer Kunden mit besseren und sicheren Banking-Service dienen.

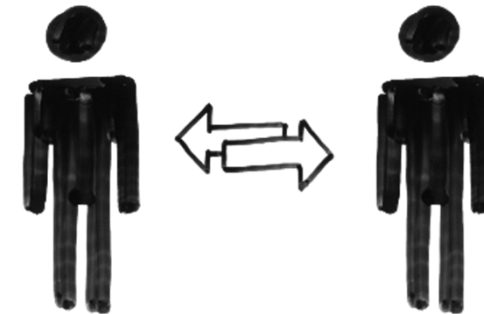
Warnung:: Bei Nichtbeachtung aktualisieren Sie Ihre Kontodaten können kann dazu führen, verändertem Einschränkung beim Einkaufen auf unserem Portal.

[Aktualisierung Ihre Informationen](#)

Zum erneuten sichern Ihrem Konto, nur bestätigen Sie Ihre persönliche Informationen.



Drei wichtige Trends sind gegenläufig zum Bedarf nach Informationssicherheit im Gesundheitswesen





Mobiles Arbeiten bietet viele Vorteile, verwischt aber auch die Grenze zwischen Geschäft und Privat





Was im privaten ja noch lustig ist, kann im Gesundheitswesen bereits heikel sein

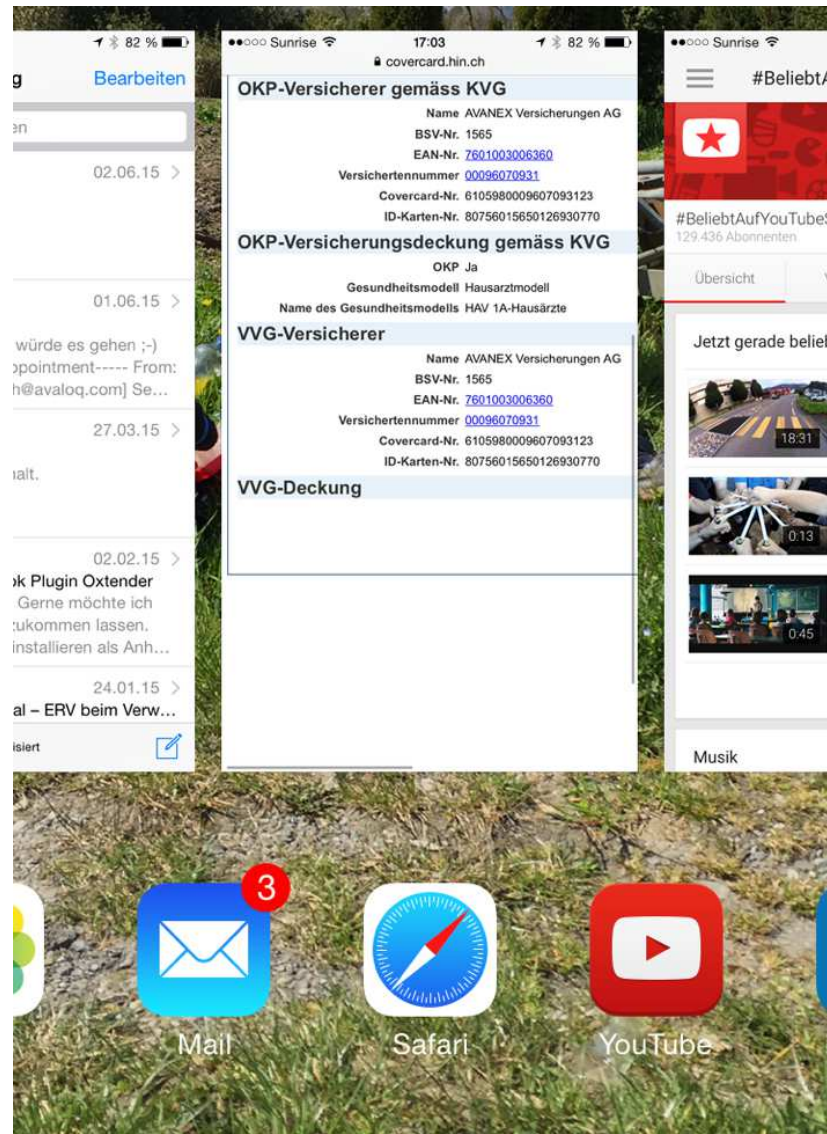


The screenshot shows a mobile browser interface with a blue header bar. The header contains a hamburger menu icon, the text "Google Web & App", a search icon, a calendar icon, a vertical ellipsis icon, a grid icon, a red notification bubble with the number "1", and a profile picture of a man with glasses. Below the header, there is a list of search history items, each with a checkbox on the left and a timestamp on the right. The items are:

- 20. Juli 2014
- Gesucht nach [boogaboo sonnenschutz](#) 22:15
- Gesucht nach [busplan mailand](#) 22:15
<http://www.touristinfo.it/index.php?PID=339>
Tickets und Preise für Metro und öffentliche Verkehrsmittel in ...
[milano24ore.de](#)
- Gesucht nach [Giardini Pubblici](#) 22:09
- Gesucht nach [fisher price formel fernsteuerung schaltet nicht ab](#) 15:56



Die Folge von «bring your own device» ist ein Zugriff mit nicht kontrollierbaren Geräten auf sensible Daten

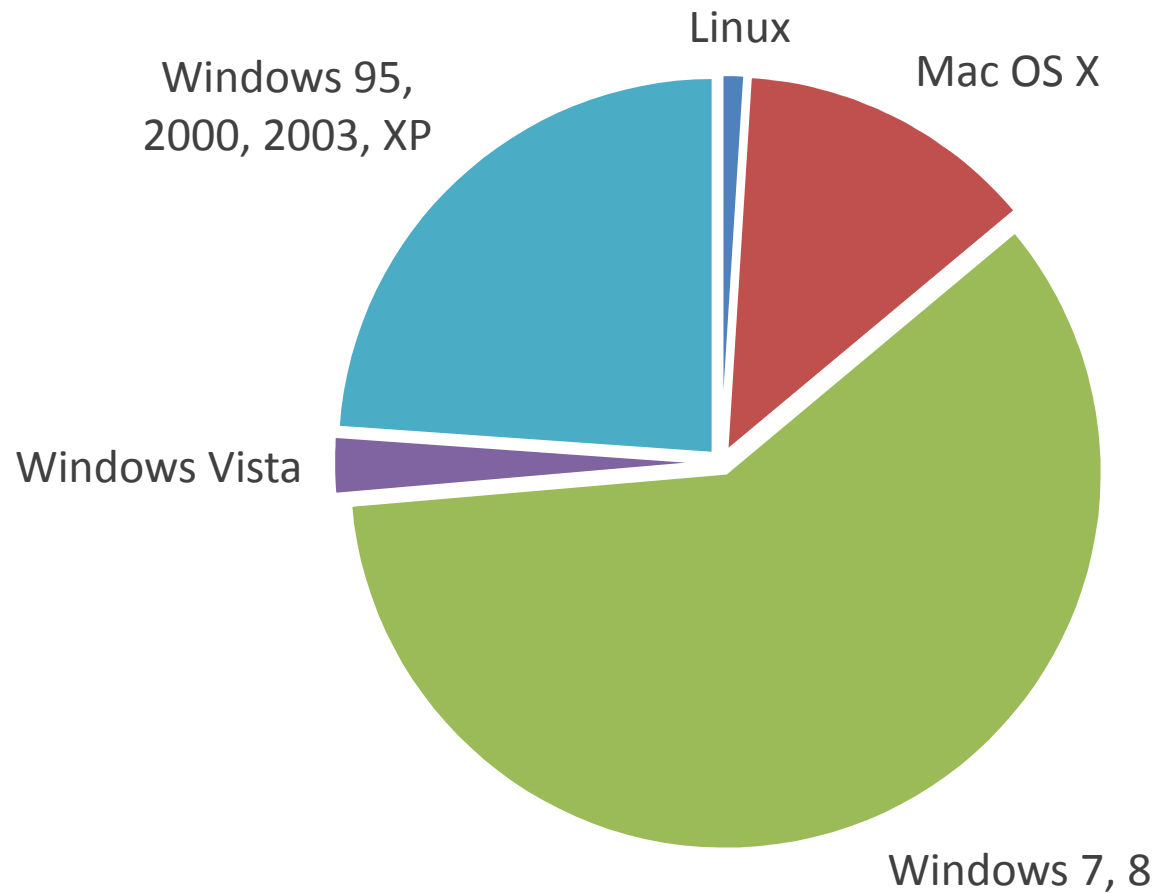




Die Devices – Zugangspunkte sind auch sonst, speziell im ambulanten Gesundheitswesen, ein Schwachpunkt

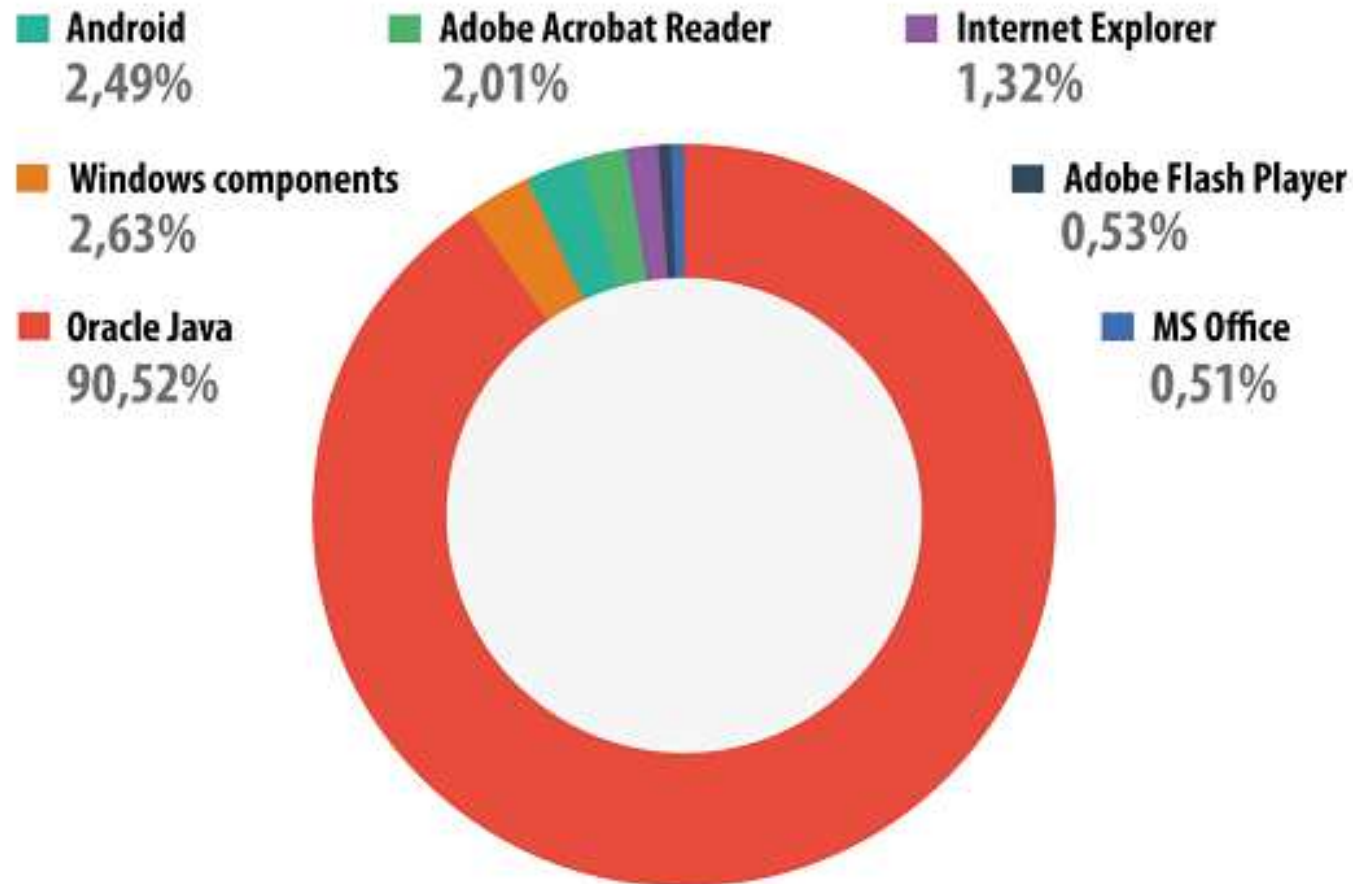


Verteilung Betriebssystem-Typ (HIN Plattform)





Internet der Dinge: Smart devices überall, viele basieren auf Java



Von Cyberkriminellen ausgenutzte angreifbare Anwendungen
Studie von Kaspersky Lab 2014

<http://www.viruslist.com/de/analysis?pubid=200883873#p1>



Gesundheitsfachpersonen vernetzen sich heute via Cloud - wenn intern nicht möglich, eben übers Mobile





Wenn sich Personen via HIN vernetzen, dann ist die Authentizität gesichert - nicht ganz ohne Aufwand



Als HIN-Teilnehmer seit vielen Jahren ... bin ich etwas erstaunt über Ihren Wunsch nach „regelmässigem“ **Nachweis meiner Identität inklusive Ausweiskopie.**

Sie verlangen dies in einem **kurzen Brief mit Hinweis auf Datenschutzstandards.**

Ich fände es nur gerecht...dass auch ich die **Identitäten mit Ausweiskopie aller Ihrer Mitarbeiter** zur meiner Verfügung habe.



Auch bei den Bedrohungen sind klare Trends festzustellen – Cybercrime geht in die Cloud!



Trends for 2015 in Cybercrime

- **Botnets move to mobile and the cloud**
- Adware becomes mainstream
- **Hacktivism goes mobile**
- **Internet of Things gets hit**
- DDoS attacks continue
- **Attacks on the cloud**

Report Alcatel-Lucent's Motive Security Labs

<http://www.esecurityplanet.com/mobile-security/16-million-mobile-devices-infected-with-malware.html>

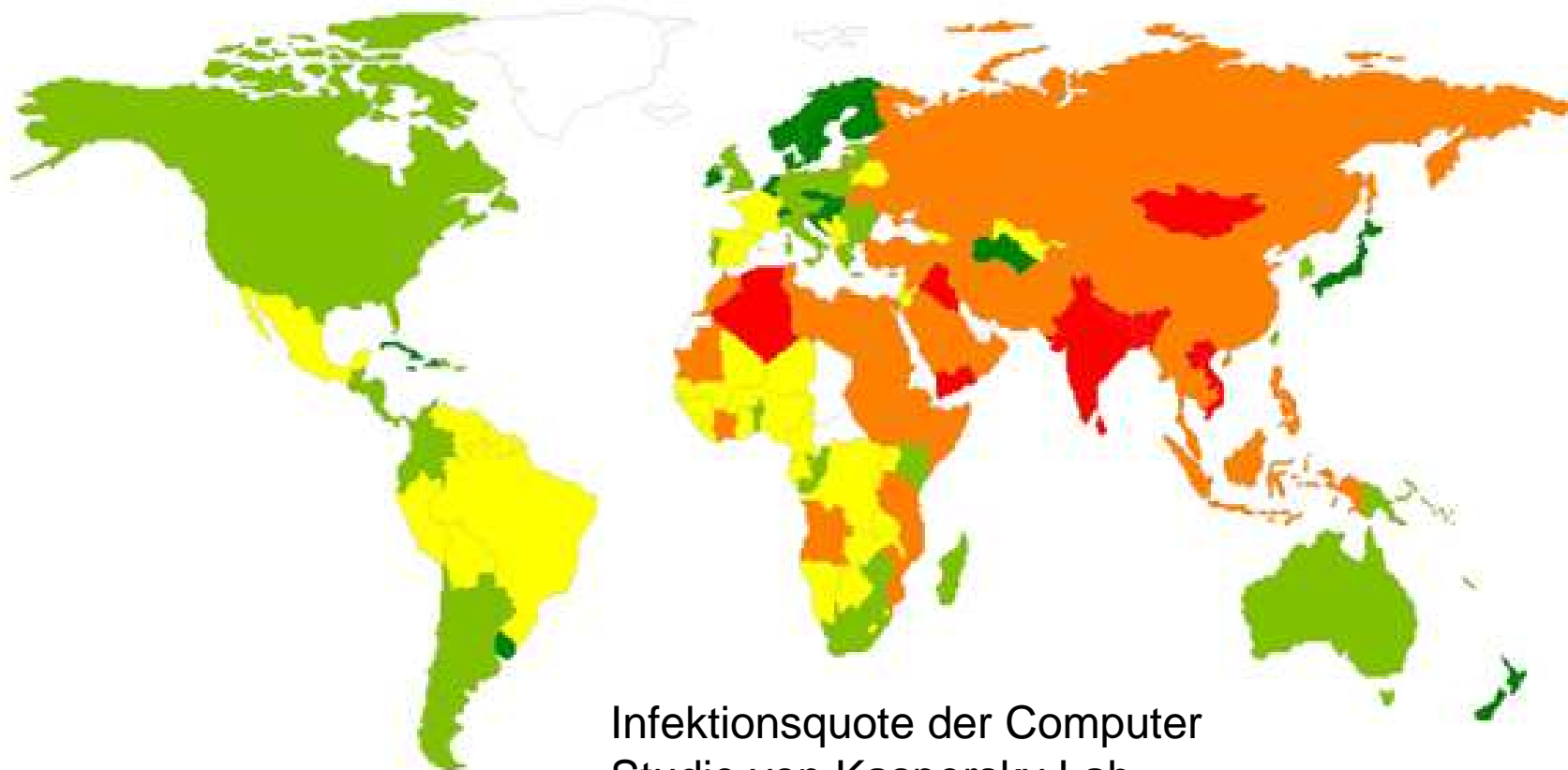


Grenzen der Machbarkeit – was können wir überhaupt machen





Mit Schadsoftware infizierte Computer ein immer grösser werdender Schwachpunkt



Infektionsquote der Computer
Studie von Kaspersky Lab

<http://www.viruslist.com/de/analysis?pubid=200883873#p1>



© Kaspersky Lab

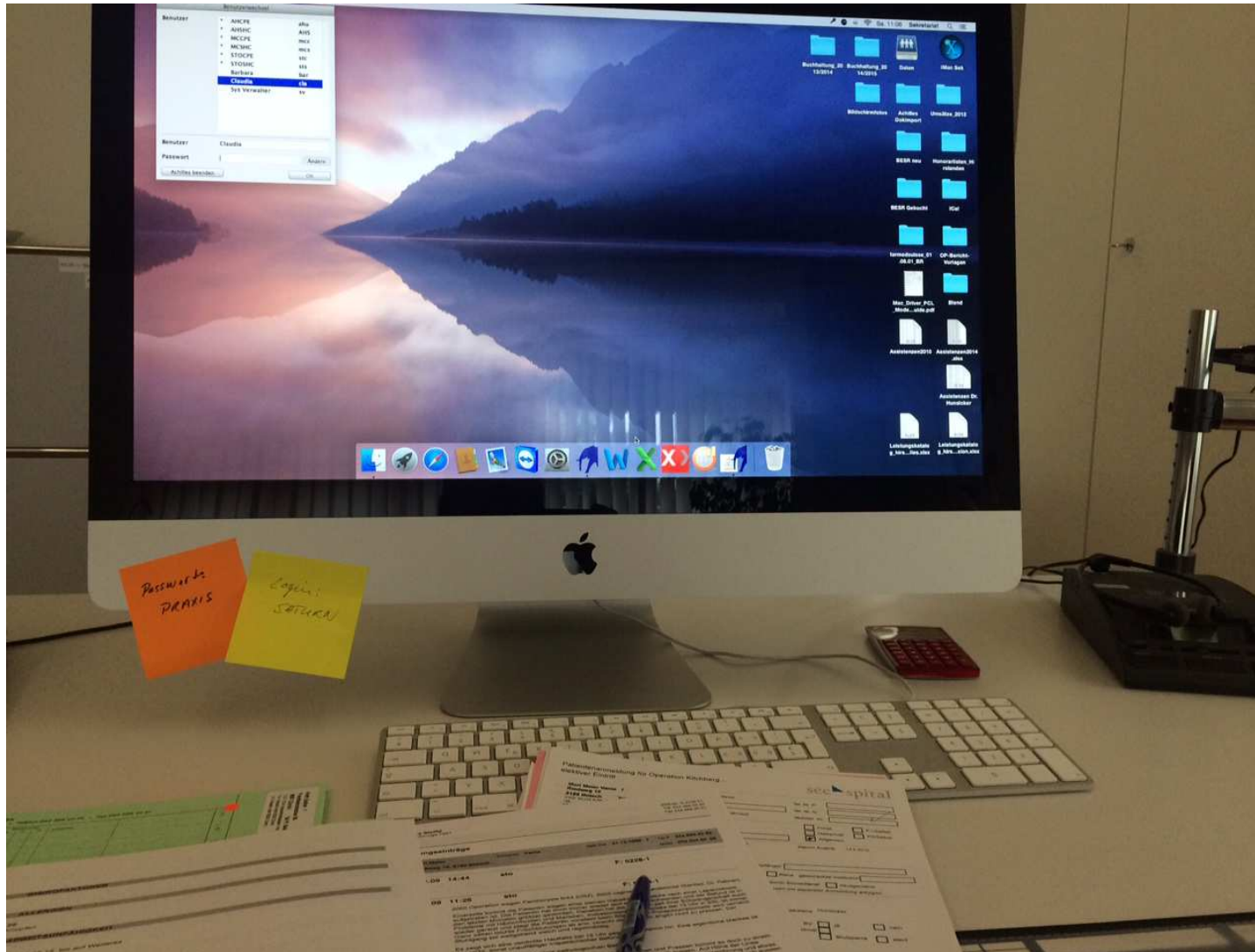


Grenzen der Machbarkeit – Massnahmen sind nur so wirksam wie das schwächste Glied in der Kette





Grenzen der Machbarkeit – Massnahmen sind nur so wirksam wie das schwächste Glied in der Kette



© U. Stoffel



Solche Pannen können überall passieren...auch im Schweizer Gesundheitswesen



Bilans de santé en balade sur le net

GAFFE — Des données médicales ultraconfidentielles de patients romands ont été librement accessibles durant des jours sur Internet. Le [REDACTED] déplore une erreur humaine.

Par [Raphaël Pomey](#) . Mis à jour le 08.04.2015
[5 Commentaires](#)





Massnahmen zur Informationssicherheit: Investieren wir am richtigen Ort?



Organisation, nicht Technik

Im Zusammenhang mit dem Einsatz von Informations- und Kommunikationstechnologien (IKT) gelte es zu beachten, dass die überwiegende Zahl der Sicherheitsvorkehrungen nicht technischer, sondern organisatorischer Art seien...

Die Hauptverantwortung für die Sicherheit beim Einsatz von IKT liege bei den Leistungsbezügern.

Die Leistungserbringer wiederum hätten die Sicherheit der Systeme im Betrieb zu gewährleisten. Zudem sind verstärkte Kontrollen und Prüfungen der Sicherheitskonzepte der einzelnen IKT-Mittel geplant.

NZZ-Artikel, März 2014 zum neuen Bundesgesetz zur Informationssicherheit



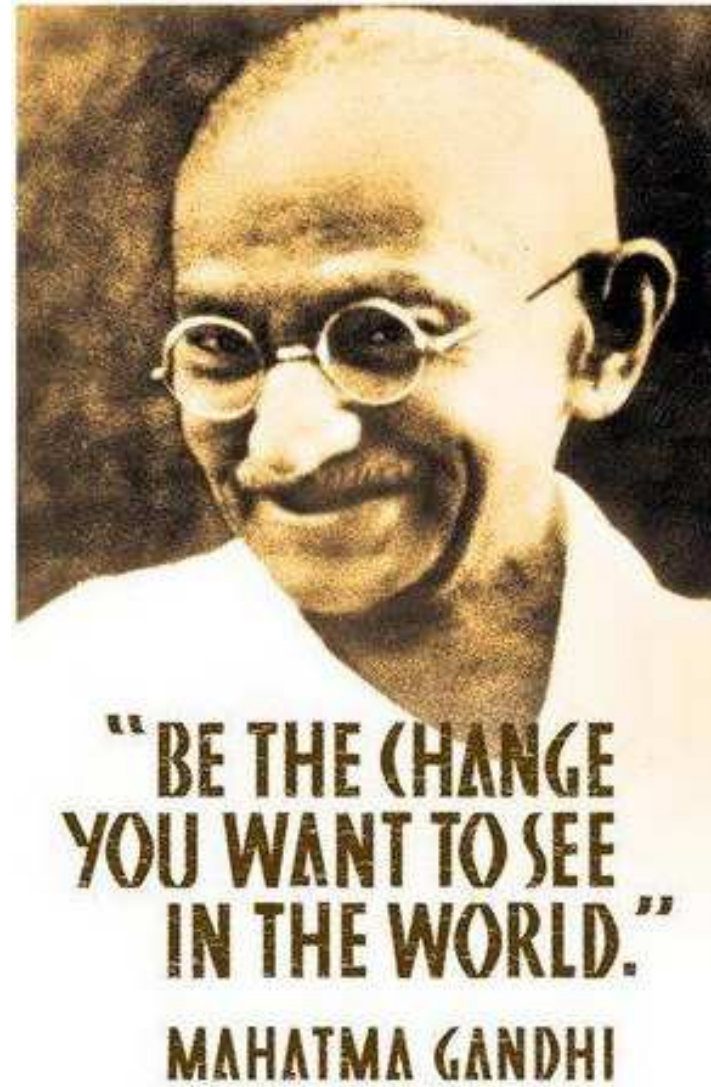
Die fehlende Verantwortung beim Einzelnen ist vermutlich ein soziokulturelles Problem der Gesellschaft



<http://wtf.300575.de/und-die-merkel-hat-echt-geglaubt-dass/>



Hoffnung für einen achtsameren Umgang mit Daten
bietet der Trend «digitale Selbstbestimmung»

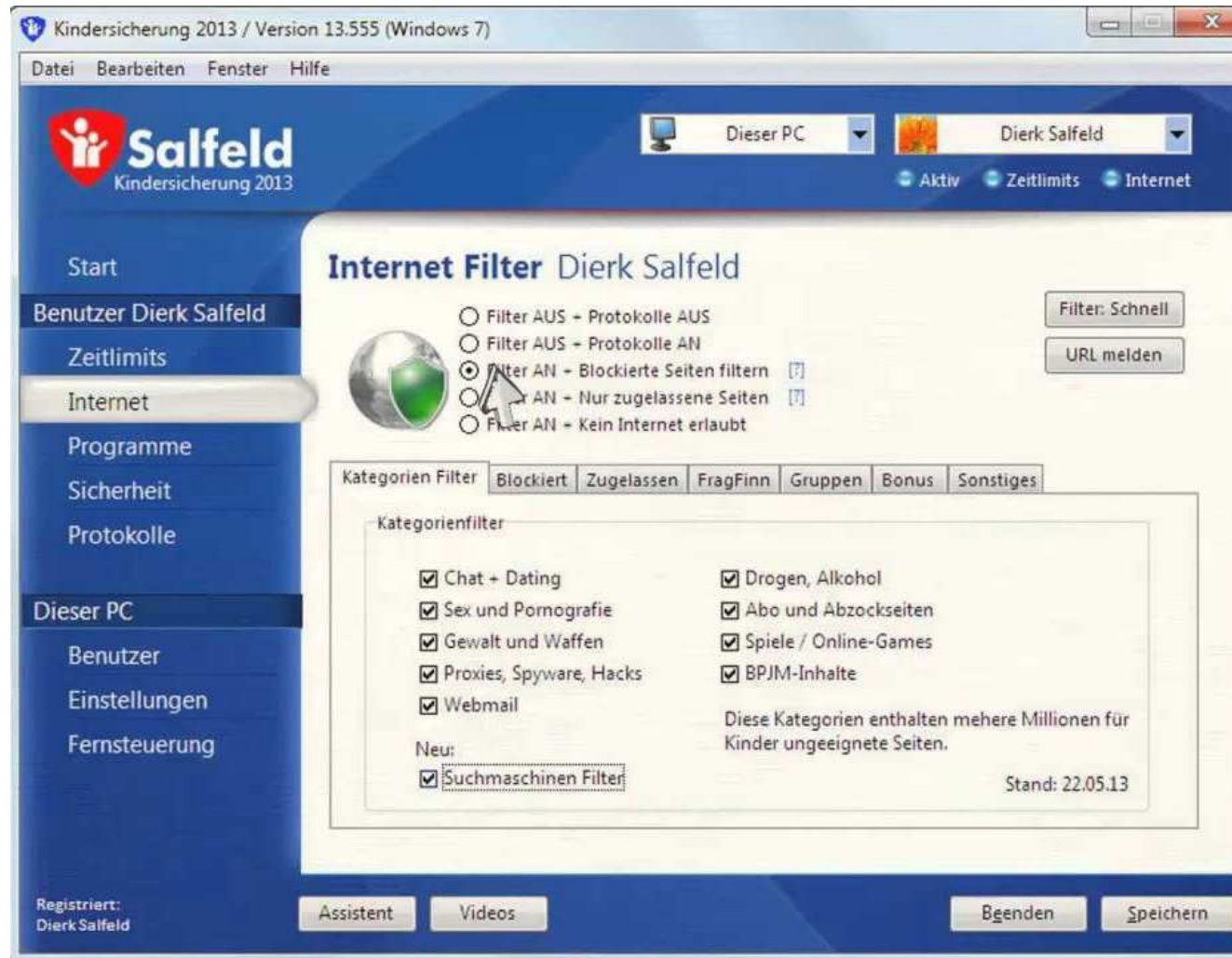




Awareness zuerst



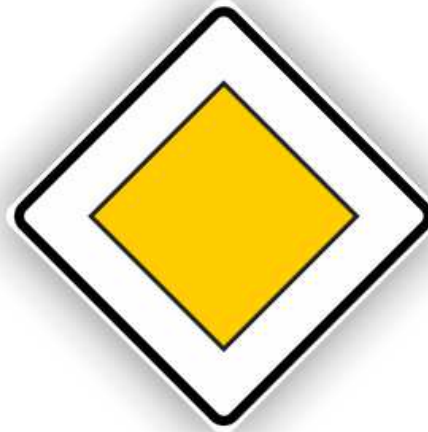
Anfang aller Massnahmen zum Schutz von Informationen muss die Awareness sein



<http://www.spezido.de/kinder-schutz-pc-software-sicherung-programm>



IT-Security als Enabler nicht Verhinderer – Massnahmen im 3-er Paket

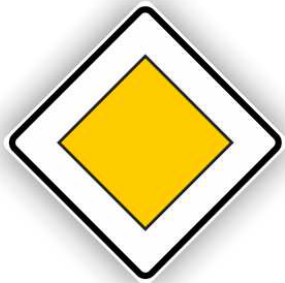




Am Beispiel Secure Mail und Schutz für Malware sieht das wie folgt aus



- Datenschutz != Virenschutz
- Auch verschlüsselte Mails können Viren enthalten



- Mails werden innerhalb der Community automatisch verschlüsselt.
- Dies bedingt zusätzliche Schutzmassnahmen, da auch Malware verschlüsselt wird.



- Auf keinen Fall merkwürdige Anhänge öffnen
- Kein Versand von ausführbaren Dateien



Awareness zuerst



An Stelle von gehärteten Geräten, sind für die heterogene IT im Gesundheitswesen andere Lösungen notwendig





100% Sicherheit gibt es nicht – wir als Provider bleiben mit unseren Grundsätzen trotzdem immer dran



- Risiken erkennen und minimieren
- Über die richtigen Informationsquellen verfügen und die Szene entsprechend beobachten
- Die richtigen technische Massnahmen umsetzen und pflegen – up to date bleiben
- Security-Awerness der Mitarbeitenden, Partner und Lieferanten immer proaktiv steigern
- Alles tun um nicht in den Fokus zu geraten



Der Wechsel vom Papier ins überall verfügbare elektronische Dossier braucht Aufklärung und Begleitung



Rockethealth © helmedica

Zur Verfügung gestellt vom Inst. für Praxisinformatik



Vielen Dank für Ihre Aufmerksamkeit

