Einblicke in die Agenda eines CISOs

Impuls-Vortrag

Frankfurt am Main, 24.11.2017

Inhalt

Zur Person

- **Chief Information Security Officer (CISO) bei paydirekt GmbH**
- vormals Berater für IT-Security und Datenschutz

- **Wirtschaftsinformatiker**
- ISACA Certified Information Security Manager (CISM)
- ISACA Certified Information Systems Auditor (CISA)

Die paydirekt

SICHER

- paydirekt ist als branchenweite Kooperation das Online-Bezahlverfahren der deutschen Banken und Sparkassen
- Hohe Vertrauenswürdigkeit, da Angebot der Hausbank oder -Sparkasse
- Rechtssicherheit durch Standort in Deutschland
- Kundenindividuelle Daten bleiben in Deutschland – es gelten die strengen deutschen Datenschutzgesetze
- Unter der Kontrolle der deutschen Finanzaufsicht
- Bekannte 2-Faktor-Authentifikation

EINFACH

- Einfacher Login
- Transparenz über paydirekt-Transaktionen z.B. durch verständliche Übersichten und Alert-Funktion für Käufer
- Einfache Händleranbindung durch hohe Kompatibilität zu heutigen Marktinfrastrukturen

DIREKT

- Potenzieller Zugang zu über 50 Mio. online-bankfähigen Girokonten und damit neue Umsatzchancen für Händler
- Einziges direkt mit dem Girokonto verknüpftes Online-Bezahlverfahren ohne zwischengeschaltete Drittanbieter

Unsere Argumente für Käufer

SICHER

- **hohe Vertrauenswürdigkeit,** da Bezahlverfahren der eigenen Bank oder Sparkasse
- **hohe Sicherheit** durch Nutzung sicherer Infrastrukturen
- **strengster Datenschutz** mit Servern von paydirekt in Deutschland
- **Anonymität** der Kunden bleibt gewahrt

EINFACH

- **hoher Komfort** durch z.B. Nutzername und Passwort reichen zur Erstanmeldung und späteren Legitimation
- die **Bezahlung** beim Online-Shopping erfolgt dann **mit nur 2 Klicks**
- Girokonto-Auszug, Benachrichtigungsfunktionen und Transaktionsjournal ermöglichen **Transparenz über Zahlungsprozess**

DIREKT

- direkt über eigenes Girokonto **ohne zwischengeschaltete Drittanbieter**
- **Käuferschutz** bei Nicht-Lieferung sowie Dispute Resolution Prozess

Inhalt

„traditionelle Regeln“

- Mindestlänge 8 bis 14 Zeichen
- Regelmäßige Passwortwechsel (zwischen 30 und 180 Tage)
- Passwortchronik - Ablehnen der letzten bereits verwendeten Passwörter
- Sperre des Benutzerkontos nach wenigen Fehlversuchen

Eine gängige Arbeitsanweisung…

„Der Benutzer hat sein Passwort geheim zu halten. Idealerweise sollte das Passwort nicht notiert werden.

Sofern die technischen Gegebenheiten dies zulassen, sind Passwörter nach den folgenden Regeln zu gestalten:

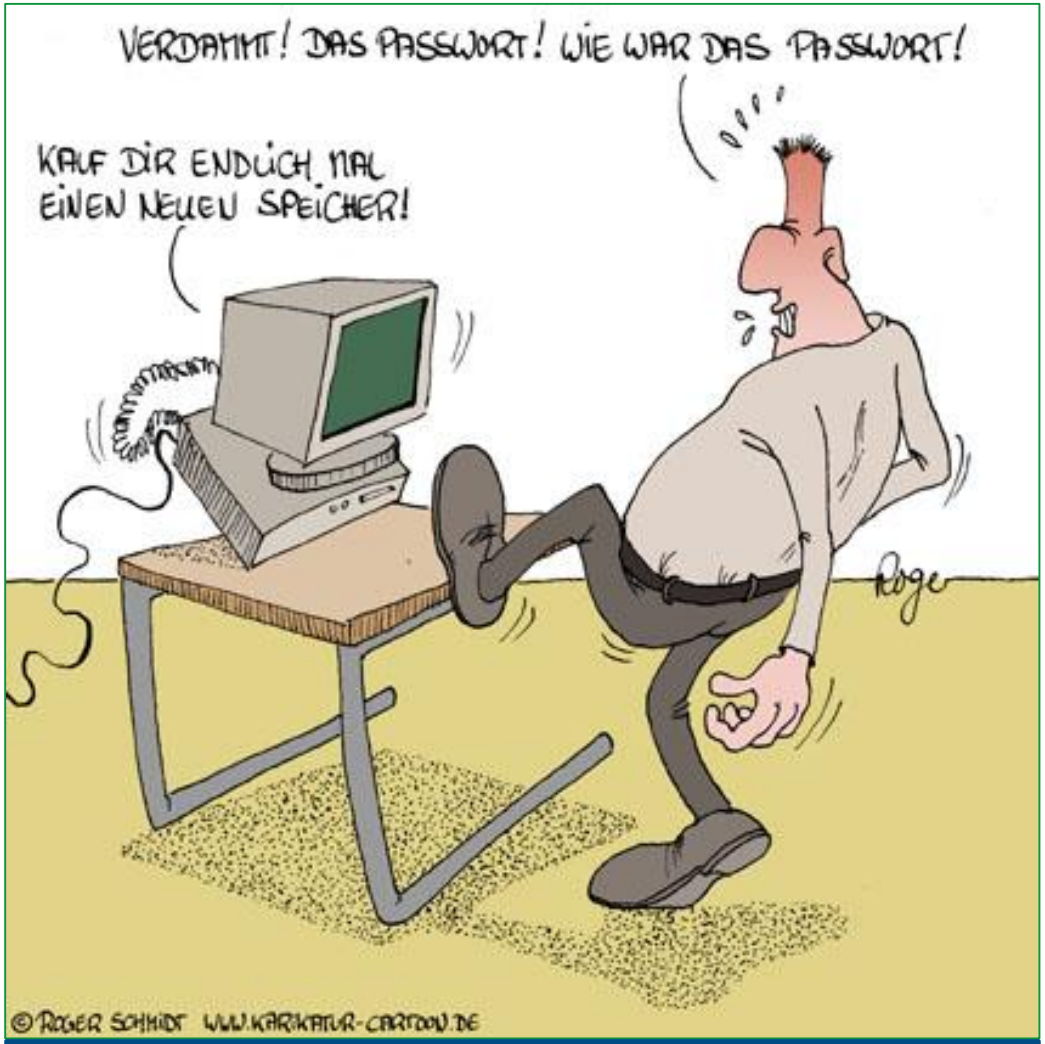
- *Das Passwort muss mindestens 8 Stellen lang sein.*
- *Das Passwort muss mindestens einen Buchstaben und mindestens eine Ziffer oder ein Sonderzeichen enthalten.*
- *Das Passwort ist regelmäßig, spätestens nach 360 Tagen, zu wechseln und sollte eine Mindestgültigkeitsdauer von einem Tag haben.*
- *Neue Passwörter müssen sich vom alten Passwort, über mehrere Wechselzyklen hinweg, signifikant unterscheiden.“*

Quelle: FU Berlin

Die gängigen Tipps von uns „Experten“

- Für jede Anwendung ein eigenes Passwort verwenden
- Keine Passwörter benutzen, die sich leicht erraten lassen.
- Passwörter ohne Sinnzusammenhang benutzen, z. B. „KaZdTs-dSsa“.
- Passende Sprichwörter oder Redewendungen helfen zum Merken von sicheren Passwörter (Bsp: „W3t,sakKvd8!“ bedeutet „Wer Exportbier trinkt, schubst auch kleine Kinder vor den Bus!“)
- Niemals Passwörter unverschlüsselt speichern, aufschreiben oder weitergeben

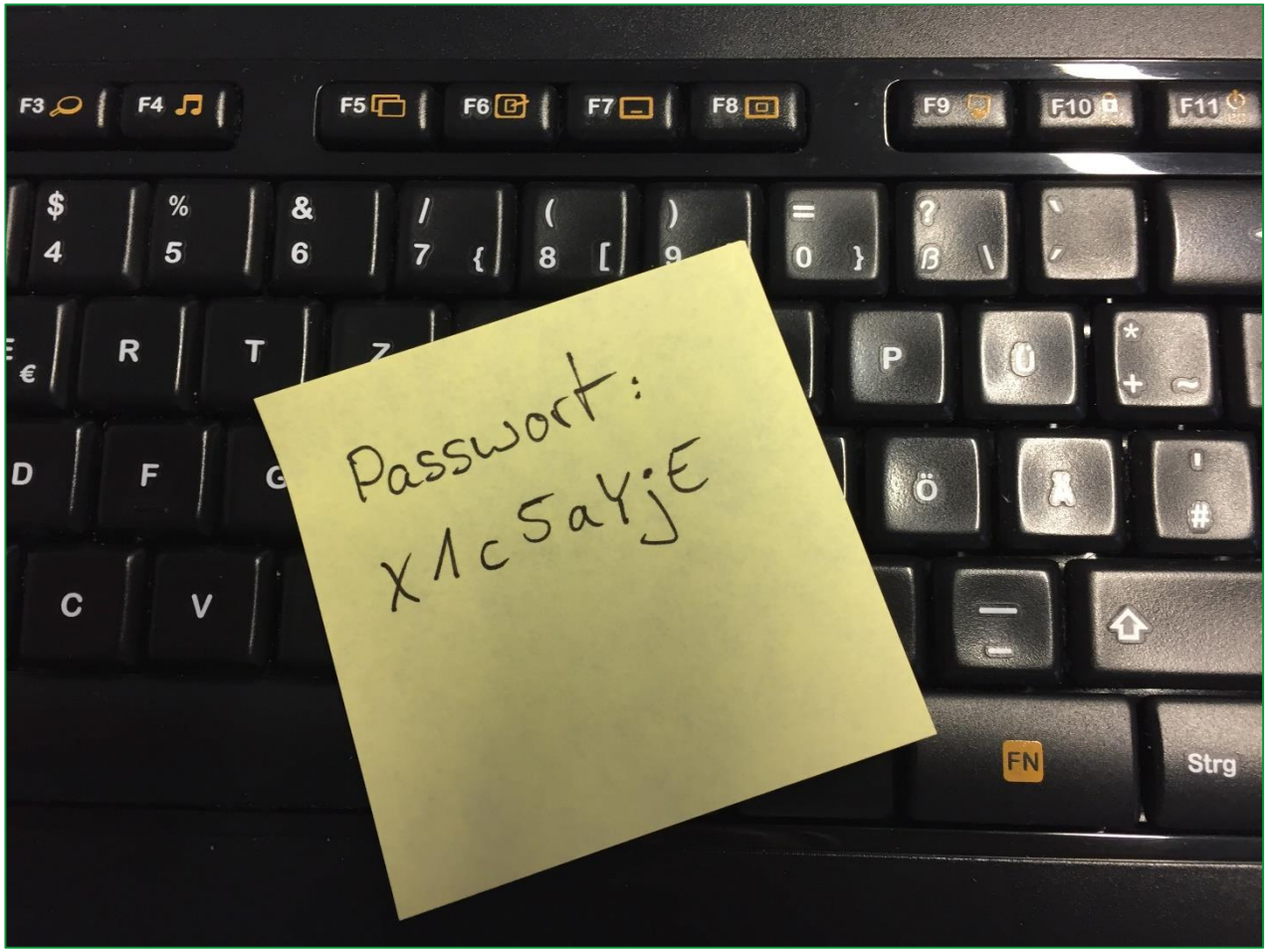
Alltagsprobleme



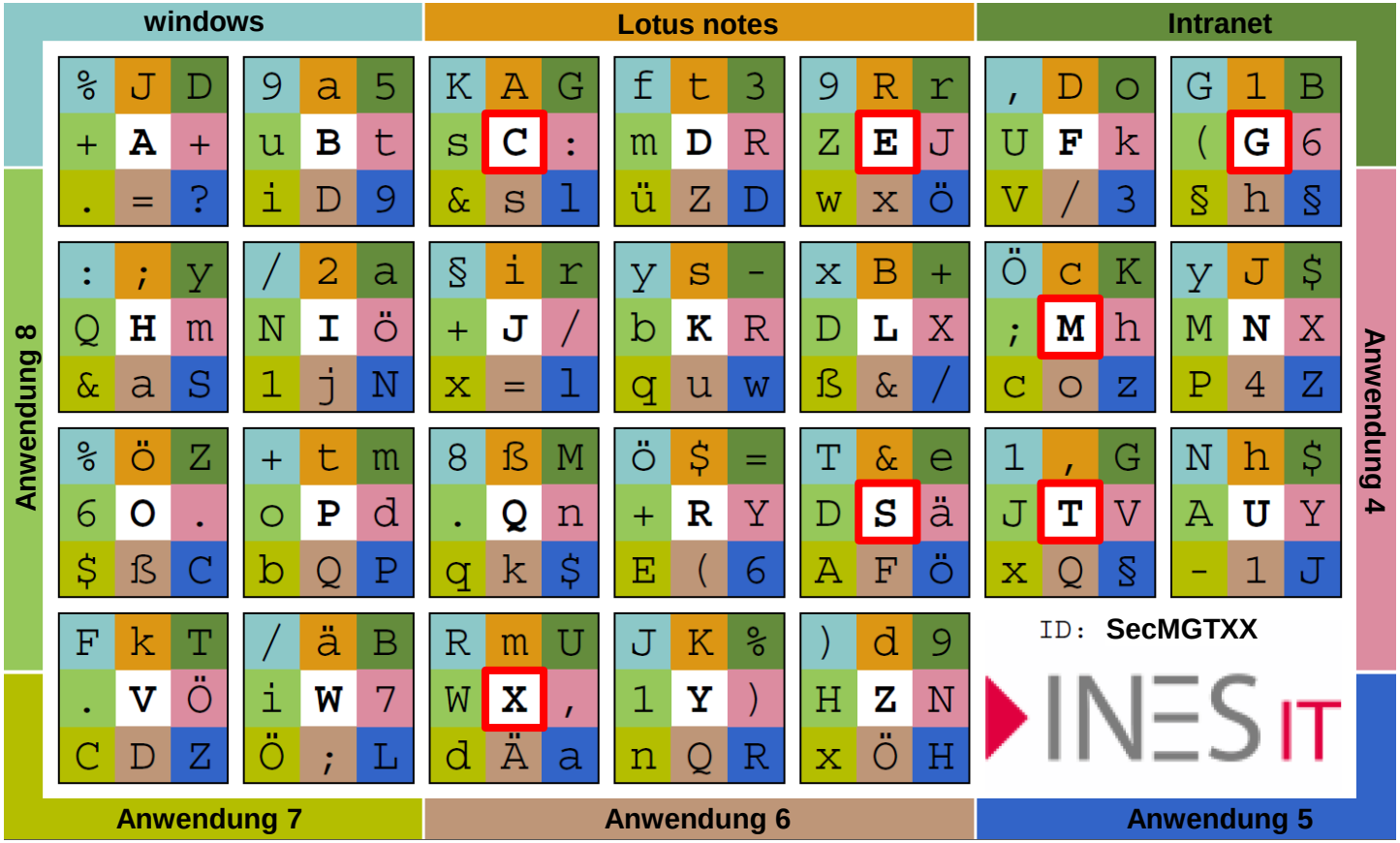
16% der Büroangestellten notieren ihr Passwort auf einem Zettel

Quelle: Infosecurity Europe, 2004

Lösungsansätze…



Lösungsansätze… Passwortkarte?!?!



Das Passwort für Windows lautet: **T9KÖG1RR**

Quelle: www.ines-it.de

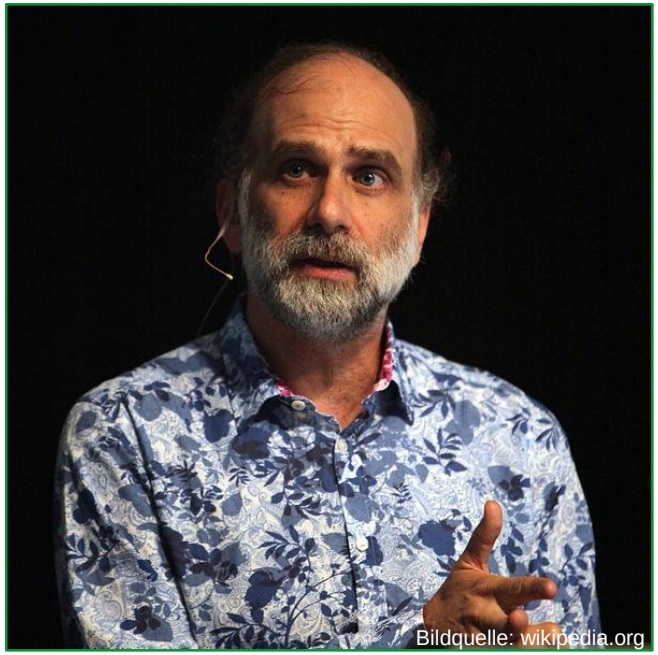
Aussagen zu den traditionellen Regeln

- *“**Never reuse a password you care about.** Even if you choose a secure password, the site it's for could leak it because of its own incompetence. You don't want someone who gets your password for one application or site to be able to use it for another.*

- ***Don't bother updating your password regularly.** Sites that require 90-day -- or whatever -- password upgrades do more harm than good. Unless you think your password might be compromised, don't change it.*

- ***Beware the "secret question."** You don't want a backup system for when you forget your password to be easier to break than your password. Really, it's smart to use a password manager. Or to write your passwords down on a piece of paper and secure that piece of paper.*

- *One more piece of advice: if a site offers **two-factor authentication, seriously consider using it.** It's almost certainly a security improvement.”*



Bruce Schneier

Quelle: https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

Aussagen zu den traditionellen Regeln

Time to rethink mandatory password changes

By: Lorrie Cranor, Chief Technologist | Mar 2, 2016 10:55AM

SHARE THIS PAGE

TAGS: Authentication | Human-computer interaction | Passwords | Research

Data security is a process that evolves over time as new threats emerge and new countermeasures are developed. The FTC's longstanding advice to companies has been to conduct risk assessments, taking into account factors such as the sensitivity of information they collect and the availability of low-cost measures to mitigate risks. The FTC has also advised companies to keep abreast of security research and advice affecting their sector, as that advice may change. What was reasonable in 2006 may not be reasonable in 2016. This blog post provides a case study of why keeping up with security advice is important. It explores some age-old security advice that research suggests may not be providing as much protection as people previously thought.

When people hear that I conduct research on making passwords more usable and secure, everyone has a story to tell and questions to ask. People complain about having so many passwords to remember and having to change them all so frequently. Often, they tell me their passwords (please, don't!) and ask me how strong they are. But my favorite question about passwords is: "How often should people change their passwords?" My answer usually surprises the audience: "Not as often as you might think."

Quelle: https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

Aussagen des NIST Special Publication 800-63B „Digital Identity Guidelines“

- Längere Passwörter erlauben
- Häufig genutzte Kennwörter blocken
- Mehr Zeichen für Benutzer
- Hashing und Salting
- Anzeige der Zugangsdaten
- 2-Faktor (keine SMS)
- Kein unnötiger Kennwortwechsel
- Auf Sicherheitsfragen verzichten
- Keine komplexen Regeln
- Keine Erinnerungen mehr

Quelle: https://doi.org/10.6028/NIST.SP.800-63b

Passwörter

- Auch „ISMS-Klassiker“ unterliegen einem stetigen Wandel
- Skepsis gegenüber den vorhandenen Regelungen sollten ein Bestandteil jeden ISMS sein

Inhalt

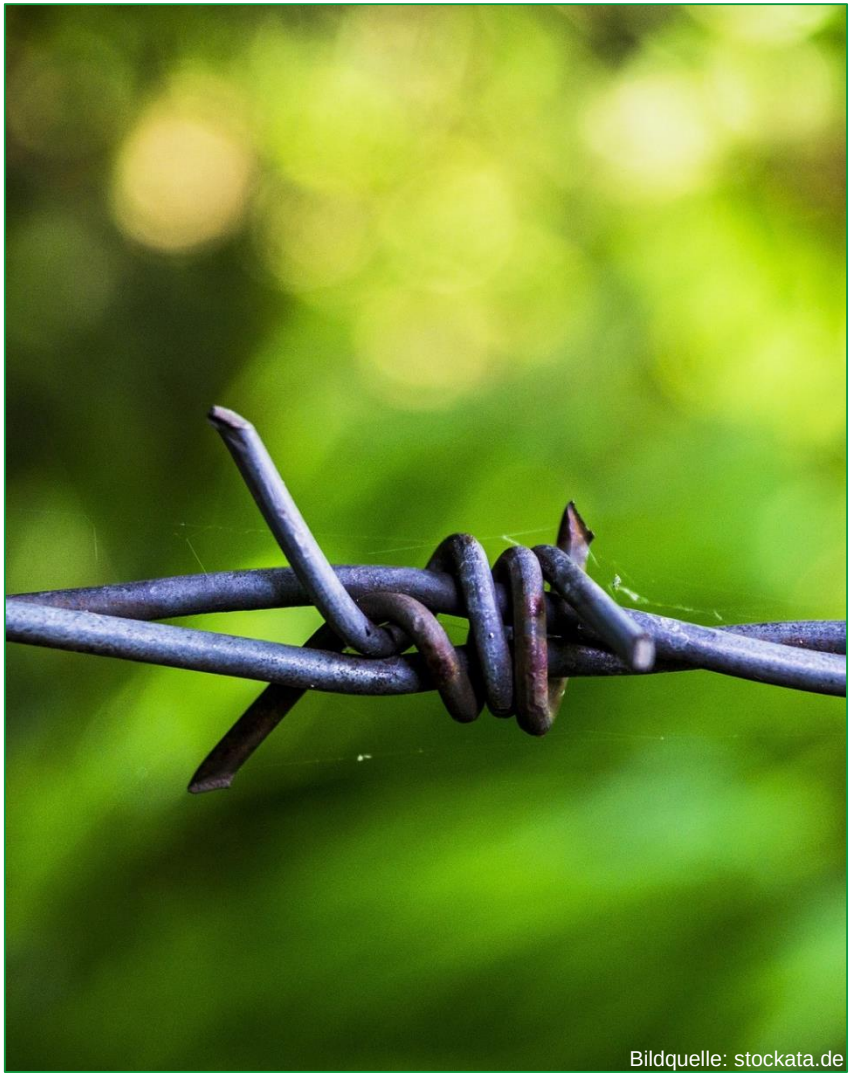
Software as a Service

„Das SaaS-Modell basiert auf dem Grundsatz, dass die Software und die IT-Infrastruktur bei einem externen IT-Dienstleister betrieben und vom Kunden als Dienstleistung genutzt werden.“

Quelle: wikipedia.de

Alltags-Beispiele für SaaS:

- Rechenzentrums-Dienste
- IT-Infrastruktur
- Online Speicher
- Büroanwendungen

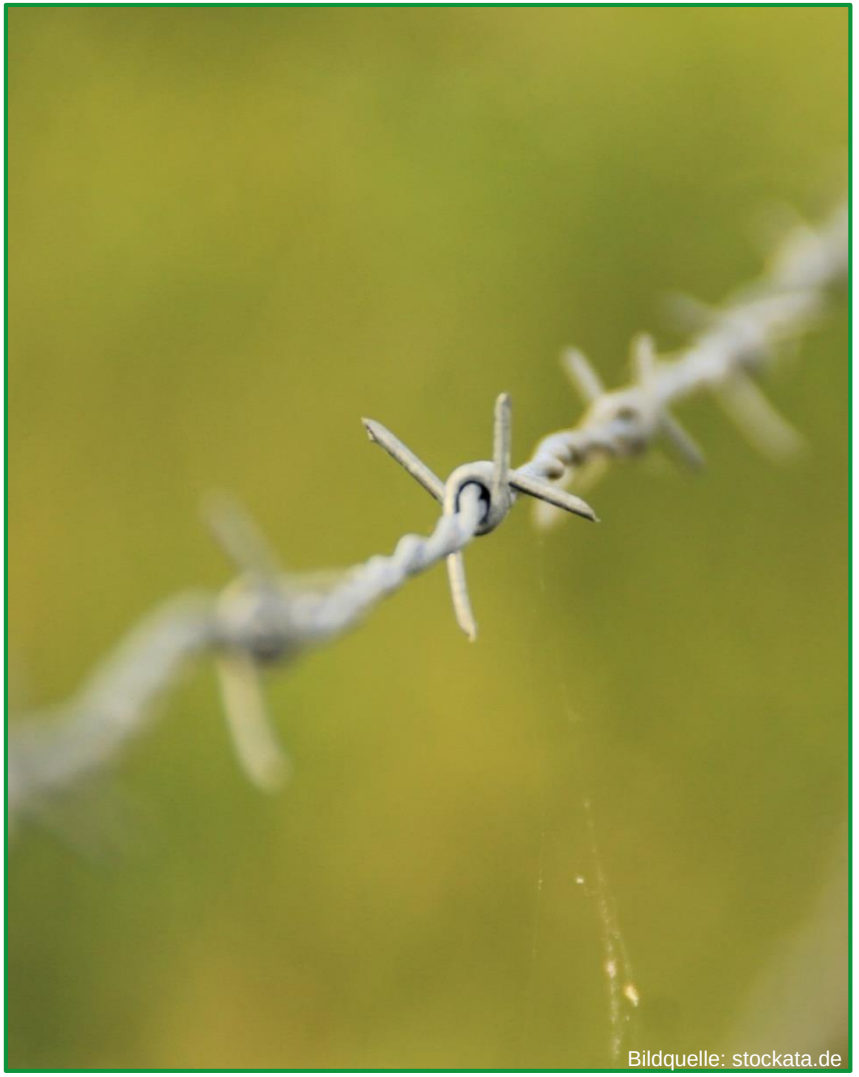


Bildquelle: stockata.de

SaaS und ISMS

„Die wichtigsten Anforderungen an SaaS-Anbieter“ (Quelle: KPMG, Bitkom):

- Hauptsitz im Rechtsgebiet der EU
- Integrationsfähigkeit der Lösungen
- Ausstiegsstrategie im Vertrag regelbar
- Transparente Sicherheitsarchitekturen/-kontrollen
- Rechenzentren in Deutschland
- Unabhängige Zertifikate
- Rechenzentren in der EU
- Mögliche Datenverschlüsselung durch Cloud-Nutzer
- Hauptsitz in Deutschland


Bildquelle: stockata.de

„SaaS-Schläfer“

Welche SaaS in ihrem Unternehmen gegebenfalls noch schlummern…

- **WhatsApp** – Kommunikation mit Kollegen & Kunden
- **Slack** – Kommunikation der Entwickler
- **Microsoft OneDrive, DropBox** – um auch zu Hause mal eine Datei zu bearbeiten
- **iCloud, Google Drive** – dienstliche Smart Phones und Tablets
- **Salesforce.com** – CRM
- Bedrohungsanalyse-Tools (z. B. Firewalls, Virenschutz, SIEM)


Bildquelle: stockata.de

ISO 27001 Annex A – A.15

- Informationssicherheitsrichtlinie für Lieferantenbeziehungen
- Behandlung von Sicherheit in Lieferantenvereinbarungen
- Lieferkette für Informations- und Kommunikationstechnologie
- Überwachung und Überprüfung von Lieferantendienstleistungen
- Handhabung der Änderungen von Lieferantendienstleistungen

Ist das vollständig geregelt und werden die Regelungen überprüft (z. B. in Audits)?

Spurensuche - ein Blick lohnt vielleicht bei…

…Firewall u. Proxy:

- Welche IPs werden regelmäßig aufgerufen?
- Welche Domains werden regelmäßig abgefragt?
- Welche Ports werden abgefragt?

…Mail-Server (ggf. Anpassen der Quarantäne-Regeln):

- Welche Mailbenachrichtigungen der Diensteanbieter werden empfangen?

…MDM-Server:

- Welche Apps sind installiert?

Bitte beachten: Es besteht Abstimmungsbedarf mit Arbeitnehmervertretern und Datenschutz, wenn die private Nutzung von Internet u. E-Mail zulässig ist!


Bildquelle: stockata.de

SaaS – ISMS-ToDos

- Überprüfen der vertraglichen Regelungen
- Auditieren der Dienstleister
- „Schläfer“ identifizieren
- Mitarbeiter für die Gefahren sensibilisieren
- Technischen Perimeter-Schutz anpassen

Bildquelle: stockata.de

Inhalt

Patchmanagement

WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm

12.05.2017 17:59 Uhr – Martin Holland, Axel Kannenberg

Screenshot der angezeigten Lösegeldforderung (Bild: Securelist)

In ganz England hat ein Kryptotrojaner am Freitag zahlreiche Krankenhäuser lahmgeleg
Und das ist offenbar nur die Spitze des Eisbergs einer globalen Welle von Infektionen mit Wana Decrypt0r 2.0 oder einfach WannaCry.

Patchday: Adobe Acrobat und Reader sind das neue Flash

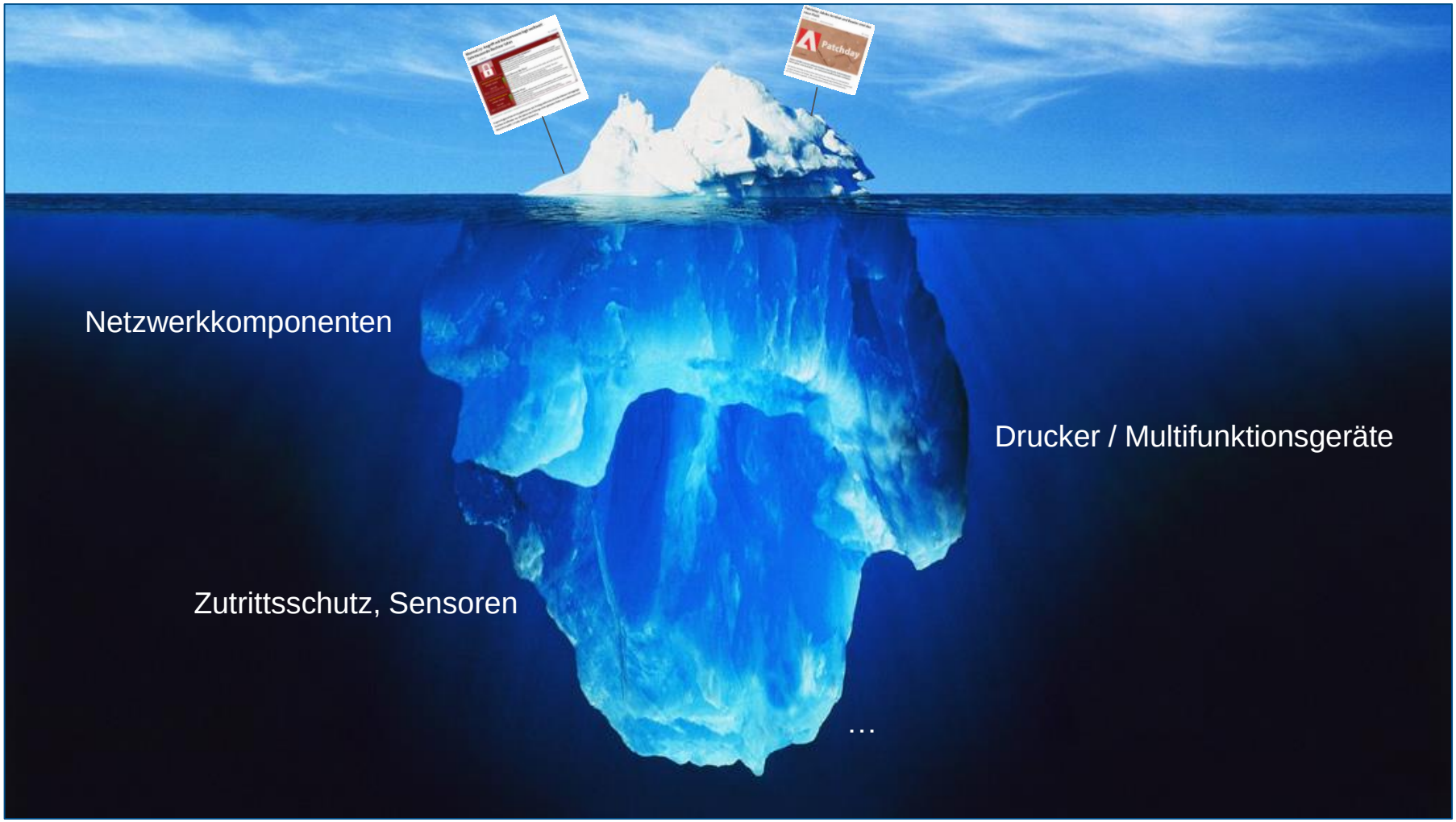
15.11.2017 10:45 Uhr – Dennis Schirrmacher

Adobe schließt in seinem Software-Portfolio einen Haufen Sicherheitslücken. Davon gelten viele als kritisch – der Löwenanteil klafft in Acrobat und Reader.

Am Adobe-Patchday im November steht nicht der Flash Player im Rampenlicht, sondern Acrobat und Reader. Die in den PDF-Anwendungen klaffendem Lücken sind 62 CVE-Nummern zugeteilt. Sicherheitsupdates stehen zum Download bereit.

Quelle: heise.de

Patchmanagement



Aktualisieren mit Bedacht…

Facebook meldet Ausfall "wegen Wartungsarbeiten"

UPDATE

26.08.2017 16:55 Uhr

vorlesen

Facebook wird täglich von rund 1,32 Milliarden Menschen genutzt. (Bild: dpa, Stephan Jansen/Symbolbild)

Am heutigen Samstag nachmittags war Facebook in vielen Ländern, darunter auch Deutschland, vorübergehend nicht erreichbar.

Das Soziale Netzwerk Facebook mit seinen täglich rund 1,32 Milliarden Nutzern in aller Welt ist am heutigen Samstag großflächig ausgefallen. Aus zahlreichen Ländern meldeten Nutzer etwa über den Kurznachrichtendienst Twitter, dass sie sich nicht bei Facebook einloggen konnten.

Quelle: heise.de

Migrationsstrategie für EOL-Produkten

McAfee
Together is power.

MENÜ

Unternehmenskunden – Startseite > Produkte >

Veräußerung von McAfee Next Generation Firewall und McAfee Firewall Enterprise

Im Januar 2016 erwarb Forcepoint™ die Geschäftsbereiche McAfee Next Generation Firewall (NGFW) und McAfee Firewall Enterprise.

McAfee Next Generation Firewall (NGFW) und McAfee Firewall Enterprise sind nun Teil von Forcepoint™.

Bitte richten Sie alle Support-Anfragen zu Next Generation Firewall und Firewall Enterprise über die entsprechende unternehmenseigene Support-Kontaktseite an Forcepoint.

Ressourcen und Informationen sind auf der Forcepoint-Website verfügbar.

Produktdetails und verwandte Ressourcen:
- McAfee Next Generation Firewall
- McAfee Firewall Enterprise

Support:
- Rufen Sie die Forcepoint-Kontaktseite für Support-Anfragen auf.

Quelle: mcafee.com

Vorausschauen und planen…

Zertifizierung: Google entzieht Symantec 2018 das Vertrauen UPDATE

vorlesen

13.09.2017 09:10 Uhr – Jürgen Schmidt

Ab April wird der Google-Browser Chrome für Zertifikate Fehler melden, die Symatecs CAs ausgestellt haben. Dazu gehören unter anderem Thawte, VeriSign, Equifax, GeoTrust und RapidSSL. Wer die noch im Einsatz hat, muss bald handeln.

Quelle: heise.de

Herausforderungen des Patchmanagements

- SPOF: Hochverfügbare und nicht redundante Systeme (z. B. Core-Router)
- Patchmanagement sollte auch „nicht präsente“ IT-Systeme
- Migrationsstrategie für End of Life (EOL)-Produkte nach Ende des Supports
- Kontinuierliche und kritische Branchenbeobachtung
- Kontrolle und Audits bei Dienstleistern

Inhalt

Persönliches Fazit

Es ist nicht immer schlecht, Schuld zu sein, denn als CISO…

- …analysieren und dokumentieren sie die schlechten Nachrichten (auch IT-Risiken genannt)
- …geben sie einer Vielzahl von Maßnahmen „ein Gesicht“, die sonst für Benutzer „gesichtslos“ blieben
- …müssen sie ihre Kollegen für Bedrohungen sensibilisieren und ggf. wachrütteln
- …schärfen sie auf diese Weise das generelle Sicherheits-Bewusstsein ihrer Kollegen
- **… ist das Teil des Jobs und zeigt die Wirksamkeit des ISMS!**

Danke für Ihre Aufmerksamkeit!

Einblicke in die Agenda eines CISOs

Christopher Ruppricht
christopher.ruppricht@paydirekt.de