Nutzer/in vs. Security

Von Vorurteilen, Stereotypen und unbewusster Inkompetenz

Katja Dörlemann
katja.doerlemann@switch.ch

Zürich, 23. Februar 2019

Unsere Aufgaben

NREN (National Research and Education Network)

Registry für .ch/.li - cc TLDs

SWITCH-CERT

22 years SWITCH-CERT – information sharing and trusted community

Customers

- Universities
- Hospitals
- Banks

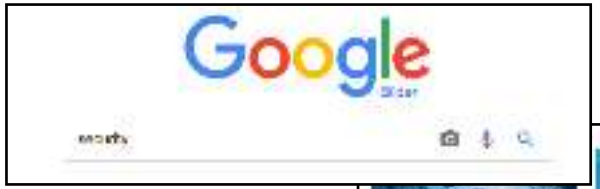
Services

Cyber Threat Intelligence, Detection, Incident and Response as core competences

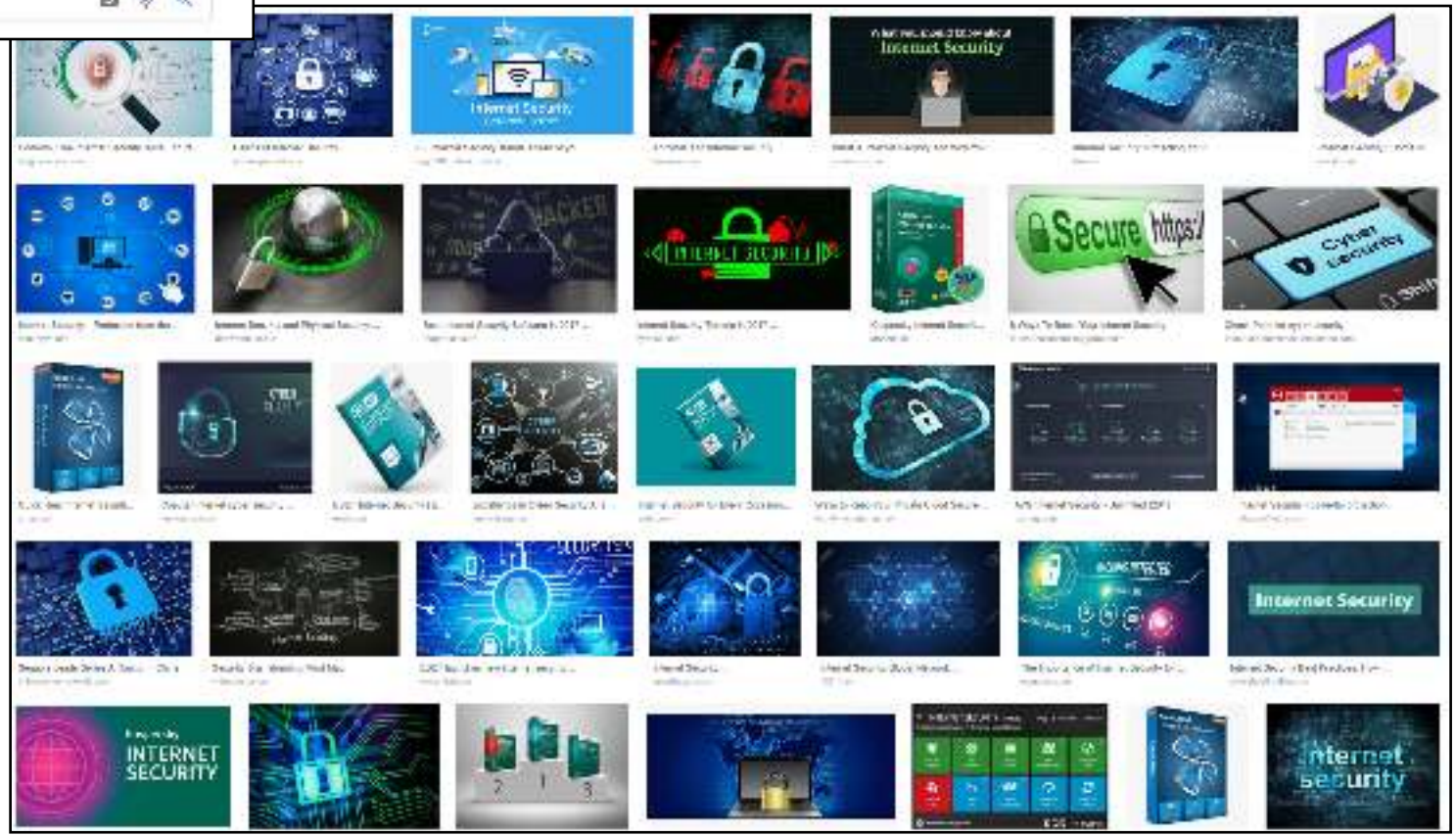
Your benefits

Comprehensive incident support and optimal network security, especially for the Swiss Internet

Nutzer/in vs. Security



21. Februar 2019, 11:30 Uhr MEZ

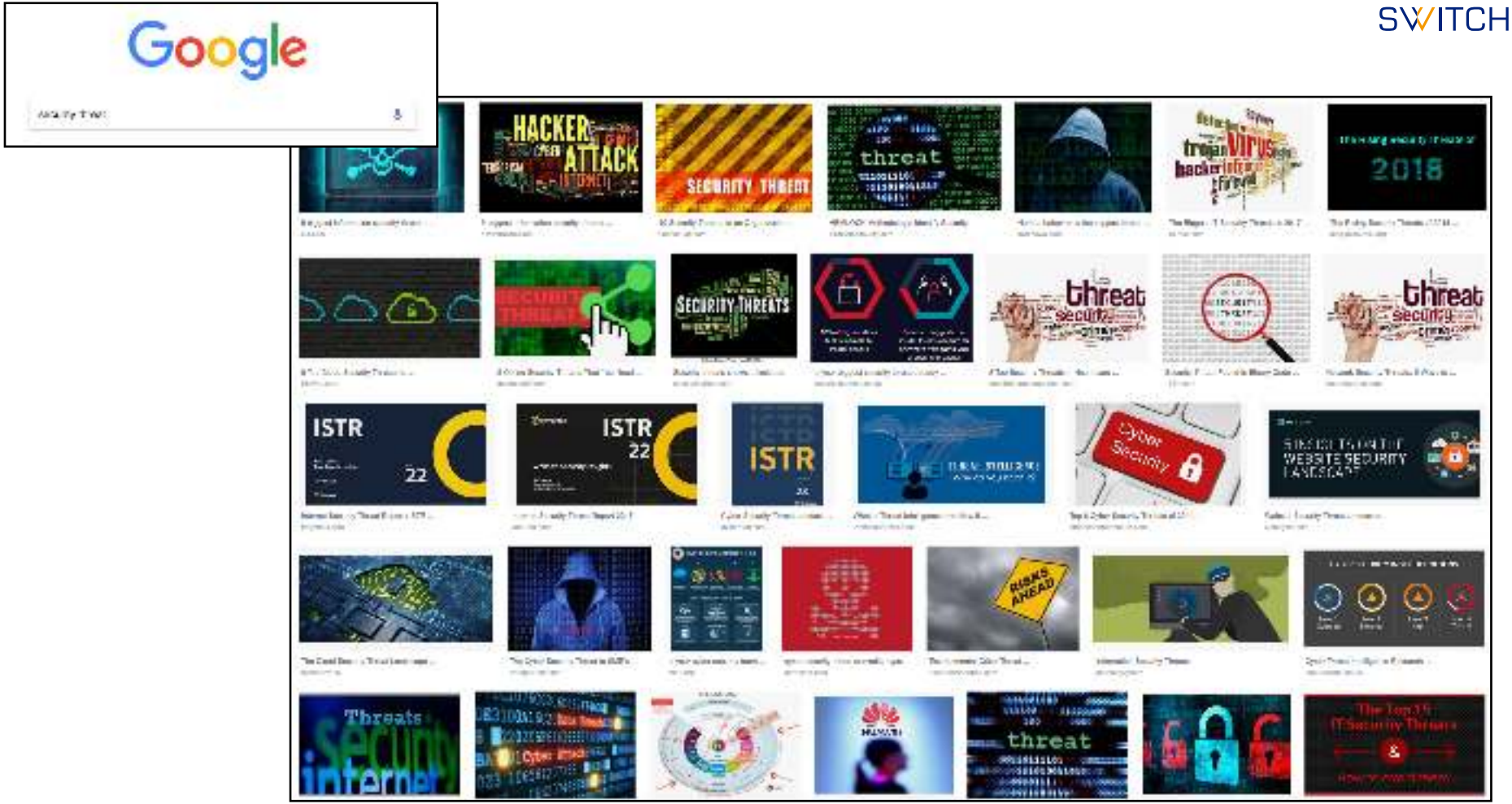


21. Februar 2019, 11:30 Uhr MEZ

21. Februar 2019, 11:30 Uhr MEZ

Blaue Schlösser

Was sind Security Threats?



21. Februar 2019, 11:30 Uhr MEZ

21. Februar 2019, 11:30 Uhr MEZ

21. Februar 2019, 11:30 Uhr MEZ

Blaue Schl🔒sser

Schwarze H👤👤dies

Der unbewusst inkompetente Typ

Der «Ich hab nix zu verbergen»-Typ

Der Panik-Typ

https://www.20min.ch/digital/news/story/Mega-Hack-mit-mehr-als-773-Mio-Mail-Adressen-31540885

SWITCH

Historischer Hack

17. Januar 2019 10:53; Akt: 17.01.2019 22:10

Datensatz mit Millionen Passwörtern entdeckt

Im Netz ist eine riesige Sammlung von Zugangsdaten aufgetaucht. Auch Schweizer Dienste und Adressen sollen betroffen sein. Das kannst du jetzt tun.

[redacted] am 17.01.2019 12:07 via

Diesen Beitrag melden

nicht mehr stand der Technik

Nein, Passwörter müssen NICHT komplex sein. Sondern lang! komplexe Passwörter sind unsicherer weil man sie sich schlecht merken kann.

[redacted] am 17.01.2019 12:46

Diesen Beitrag melden

schwierig

Fast jedes Passwort lässt sich knacken. Da macht es wenig Sinn hundert verschiedene PW zu haben, nur so nebenbei, wer soll sich die alle merken können? Aha, man schreibt sie auf, einen blöderen Ratschlag gibts höchstens noch indem man dem Nutzer rät seine Kennzahl direkt auf der Kreditkarte zu notieren. Der regelmässige Wechsel des PW ist viel wirksamer. Meine Meinung

[redacted] am 17.01.2019 13:15

Diesen Beitrag melden

Hack mich doch.....

Mit dem kann ich sehr gut leben,ich habe nicht viel zu verbergen!

[redacted] am 17.01.2019 12:41 via

Diesen Beitrag melden

mehrere Passwörter?

nützen nur bedingt,geht man z.b. mit google. ins internet,und von da aus weiter auf andere seiten haben die meisten alle Passw. gespeichert, weil man nicht jedesmal alles eingeben will.Aber müst es auch egal wenn jemand meine Mails liest,wichtig ist es mit dem Bankverkehr,und den finde ich gut geschützt mit dem Photosean.

2018 LastPass - Psychologie der Passwörter: Nachlässigkeit verhilft Hackern zum Triumph

Wir wollen Passwortrisiken nicht wahrhaben

21 %

glauben nicht, dass die Verwendung desselben oder eines ähnlichen Passworts ihre Konten bzw. Informationen verstärkt gefährdet.

21 %

Viele denken, immun gegen Angriffe oder kein Ziel zu sein

51 %

denken, dass Hacker niemals anhand von in sozialen Netzwerken preisgegebenen Informationen eines ihrer Passwörter erraten können.

51 %

Hast Du die Sache facebook gemeldet?

Nö, ist ja nix passiert. 😀

Hm, ok. Hast du dein Passwort geändert?

Neeee… 😆

🙈

Meinst Du, dass sollte ich noch machen?

2018 LastPass - Psychologie der Passwörter: Nachlässigkeit verhilft Hackern zum Triumph

Ahhhhhhh!
Wir werden alle beobachtet!
Kameras… - oh!
Ein iPhone für 100 Stutz…**klick**

2018 LastPass - Psychologie der Passwörter:
Nachlässigkeit verhilft Hackern zum Triumph

Security vs. Nutzer/in

Hacknowledge

ISSS Information Security Society Switzerland

DIGITALE GESELLSCHAFT

SWISS INTERNET SECURITY ALLIANCE

Deloitte.

SIGS Security Interest Group Switzerland

MELANI

ICT SWITZERLAND
UMBRELLA ORGANISATION FOR THE DIGITAL ECONOMY

DXC.technology

eBanking but secure!
Your guide for secure eBanking

ISPIN AG ZURICH swiss made security

pwc

COMPASS SECURITY

EY Building a better working world

swisscom

CCC-CH

swissICT

infoGuard
SWISS CYBER SECURITY

SANS

INSOMNI'HACK

black hat

DEFCON

1ST

RSA CONFERENCE

17-19 October 2017
MMXVII
HACK.LU

SWISS CYBER STORM


Network
Web
Information
Internet
DNS
Physical
Mobile
Policies
Security
Cloud
Data
Management

Was sind Security Threats?

SWITCH

Ransomware, Phishing und Co.

Der Faktor Mensch in der Cyber Security

von Alexandra Lindner - 18.04.2018

Cybersecurity PA, il "fattore umano" è il problema: lo scenario

| Facteur humain, le plus gros danger en cybersécurité ?

Il fattore umano, una vulnerabilità nei processi di sicurezza aziendale

Computerworld Breakfast Session 2018 07.09.2018, 08:47 Uhr

Faktor MENSCH - der Mitarbeiter als Einfallstor für Cyberkriminelle

Der Mensch bleibt Schwachstelle Nr. 1 bei Cybersecurity

Wie erhalten Angreifer und Kriminelle am leichtesten Zugriff auf die internen Ressourcen eines Unternehmens? Eine Möglichkeit besteht im Einsatz technischer Mittel. Es geht aber auch anders. Wie eine Befragung des BSI ergeben hat, sind die Menschen die größte Schwachstelle in IT-Sicherheitskonzepten.

Il fattore umano è il vero problema della cybersecurity

Nuovi studi confermano che il crimine informatico non prende di mira infrastrutture critiche o vulnerabilità dei software informatici, ma le persone e le loro debolezze, per il furto di denaro e dati e per stabilire le basi per attacchi futuri.

Why the human factor is an evergreen problem in cybersecurity

Employee errors in business are a critical threat to nearly half of organizations. Here's how they are trying to solve it.

Mittelstandsbotschafter

Cyber Security: Warum der Faktor Mensch so wichtig ist

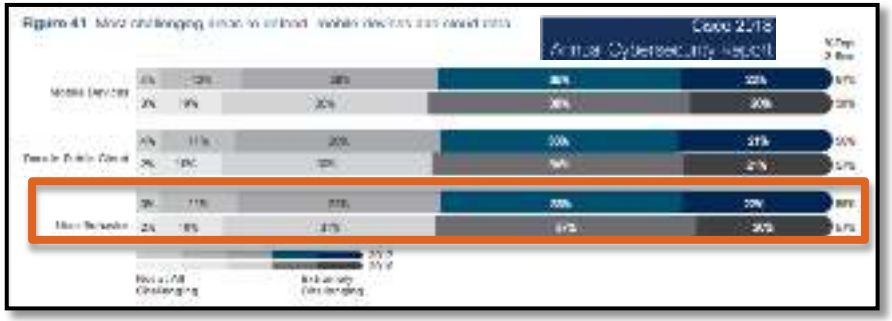
Das amerikanische Marktforschungsunternehmen Enterprise Strategy Group hat in einer aktuellen Untersuchung festgehalten, was IT-Sicherheitschefs gerade den Kopf

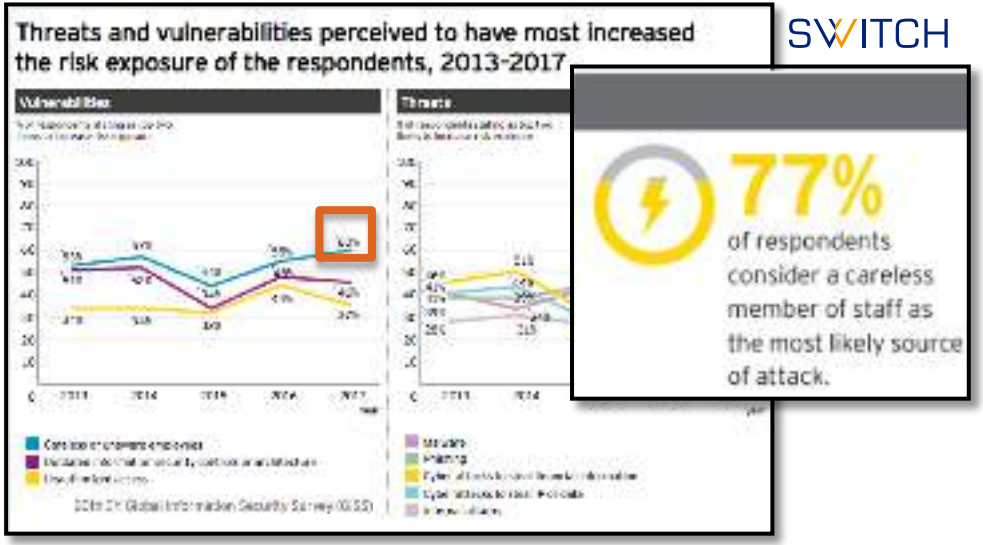
CYBERSÉCURITÉ : INVESTISSEZ LE FACTEUR HUMAIN !

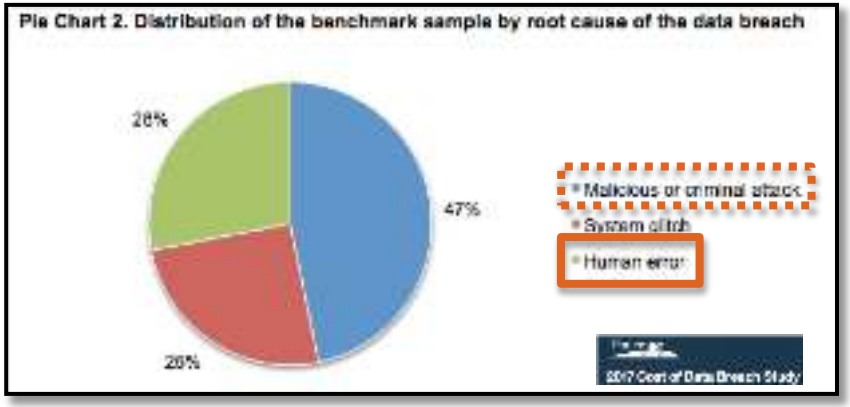
par Alain de Fooz | Nov 27, 2018 | Expérience | 0 commentaires

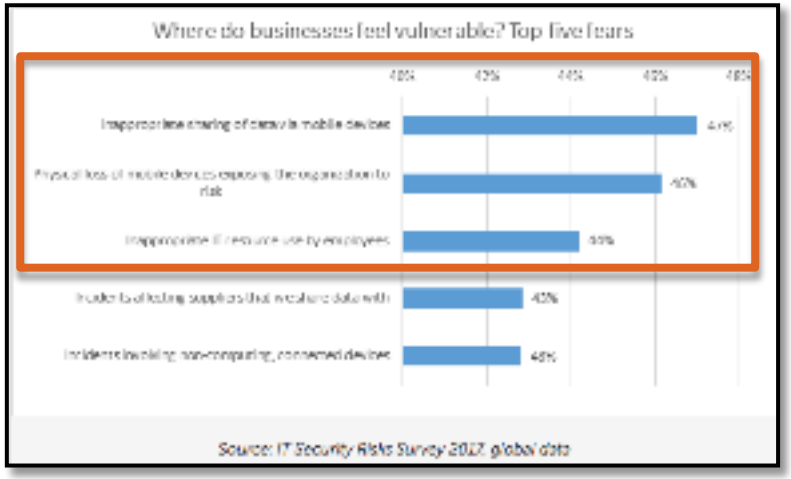
The human factor driving web application security flaws

By Pieter Danhieux, Co Founder and CEO, Secure Code Warrior




Threats and vulnerabilities perceived to have most increased the risk exposure of the respondents, 2013-2017
Vulnerabilities
Threats
77%
of respondents consider a careless member of staff as the most likely source of attack.


Pie Chart 2. Distribution of the benchmark sample by root cause of the data breach
28%
47%
25%
Malicious or criminal attack
System glitch
Human error
2017 Cost of Data Breach Study


Where do businesses feel vulnerable? Top five fears
Source: IT Security Risks Survey 2017, global data

Der Mensch bleibt Schwachstelle Nr. 1 bei Cybersecurity

Why the human factor is an evergreen problem in cybersecurity

Il fattore umano è il vero problema della cybersecurity

Blaue Schlösser

Schwarze Hoodies

SWITCH

SECURITY AWARENESS soll uns alle retten

Was ist Security Awareness?

Security Awareness is…

ISO 27000:2016:
…"[one of the] fundamental principles [that] contribute to the successful implementation of an ISMS".

OECD Guidelines for the Security of Information Systems and Networks:
…"the first line of defence for the security of information systems and networks."

NIST SP800-50:
…"not training. The purpose of awareness presentations is simply to focus attention on security."

wikipedia:
…"the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization."

Security Awareness is…

ISO 27000:2016:
…"[one of the] fundamental principles that contribute to the successful implementation of an ISMS".

OECD Guidelines for the Security of Information Systems and Networks:
…"first line of defence for the security of information systems and networks."

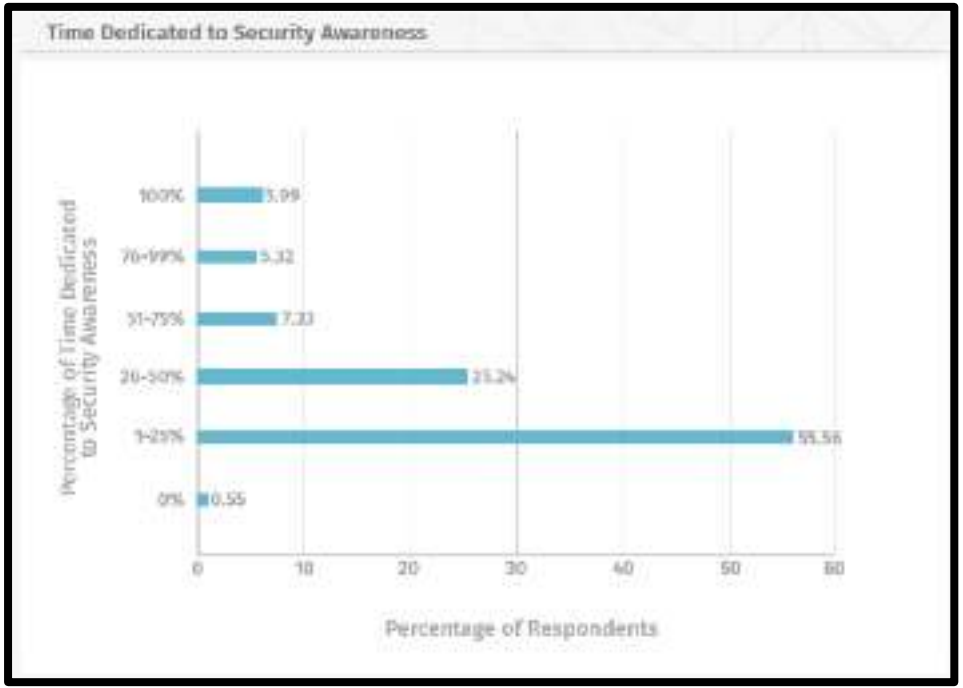
NIST SP800-50:
…"not training. The purpose of awareness presentations is simply to focus attention on security."

wikipedia:
…"the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization."

Merke:

1. Security Awareness ist sehr wichtig!
2. Security Awareness Massnahmen sollen sensibilisieren.
3. Security Awareness Massnahmen sollen nachhaltig Wissen über Informationssicherheit vermitteln.

Fig. 7 - What percentage of your time is focused on security awareness?



SANS SECURITY AWARENESS

https://www.sans.org/security-awareness-training/reports/2018-security-awareness-report
https://www.sans.org/security-awareness-training/reports/2017-security-awareness-report

AWARENESS
Aufmerksamkeit und Interesse für ein bestimmtes Thema erhöhen

EDUCATION
Neue Fähigkeiten und die Theorie dahinter lehren

TRAINING
(Neue) Fähigkeiten lehren und üben

SANS SECURITY AWARENESS

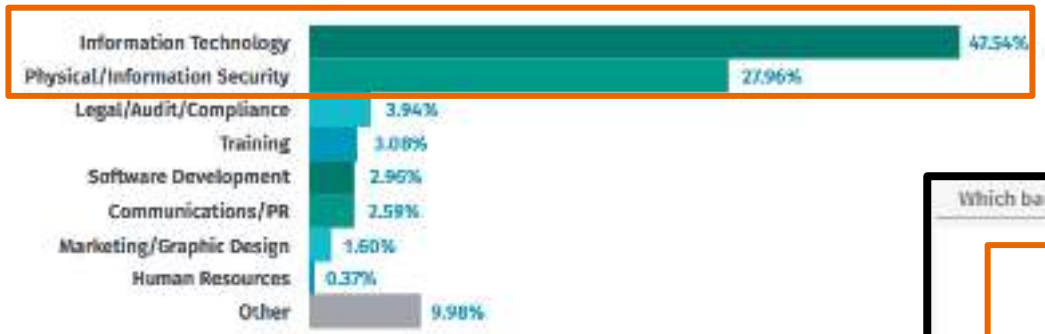
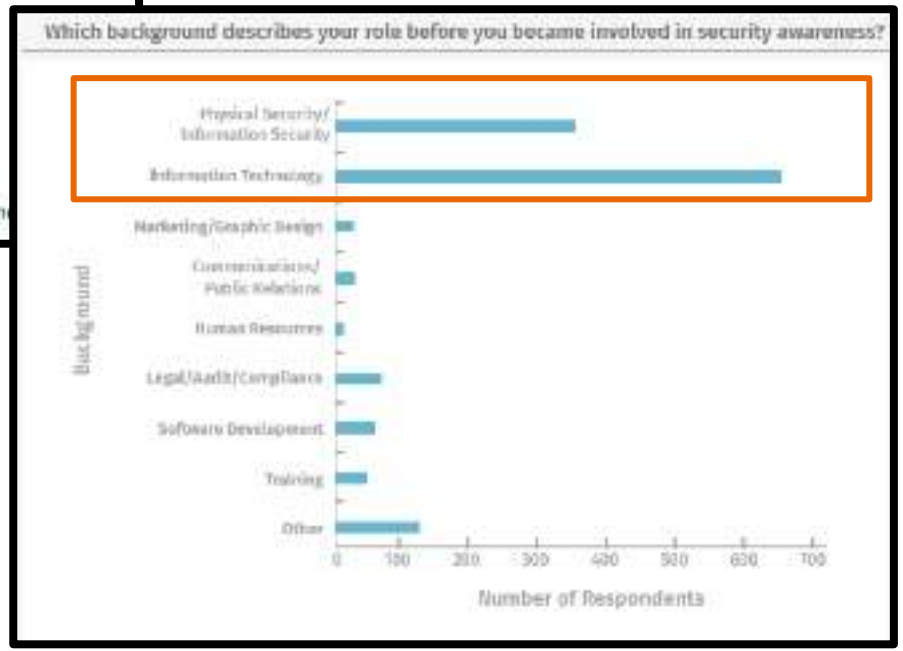


Fig. 12 - Which most closely describes your role before you become involved in security awaren



https://www.sans.org/security-awareness-training/reports/2018-security-awareness-report
https://www.sans.org/security-awareness-training/reports/2017-security-awareness-report

Der «Bitte, bitte, bitte»-Typ

Der autoritäre Typ

Der Schadenfreude-Typ

Bitte, bitte, bitte wechseln Sie
…*schnief*… Ihr Passwort.

"12345" ?!?!
Ab sofort gibt's kein Internet mehr für Dich!

HAHAHAHAHA
HAHAHAHAHA
HAHAHA !!!

> *The geeks have inherited awareness (is that good?).*

– SANS Security Awareness Report

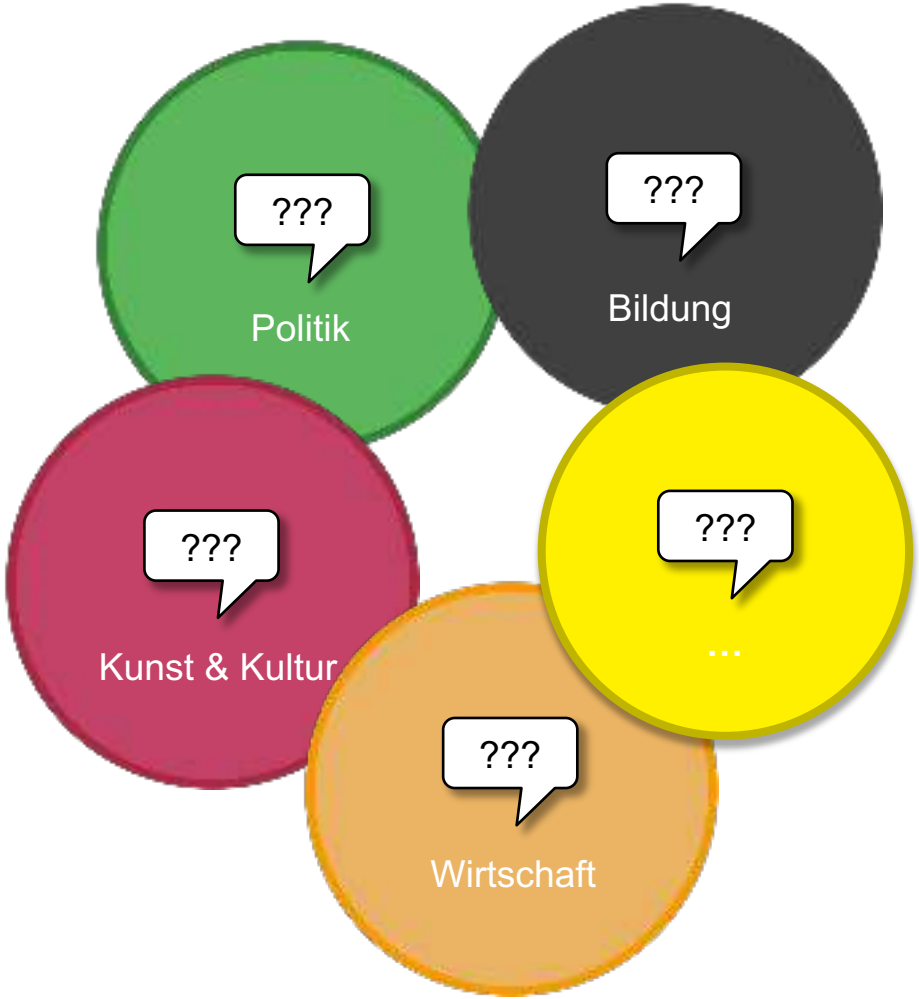

management
phishing-test
newsletter
guidelines
eLearning
event
evaluation
comic
slogan
game
policy
FAQ
audit
testimonials
presentation
socialMedia
externalPR
webpage
training
intranet
poster
quiz
sticker
coaching
storytelling
competition
video
podcast
giveaway
branding
screensaver

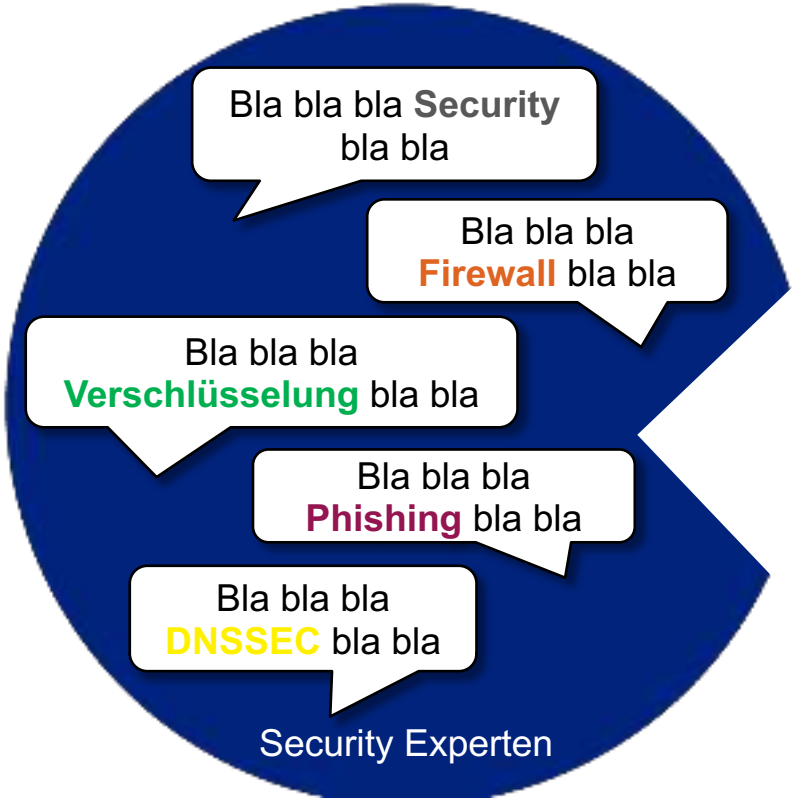
1. Fehlende Kommunikationsexpertise
2. Geringe finanzielle und zeitliche Ressourcen
3. Fehlende Unterstützung

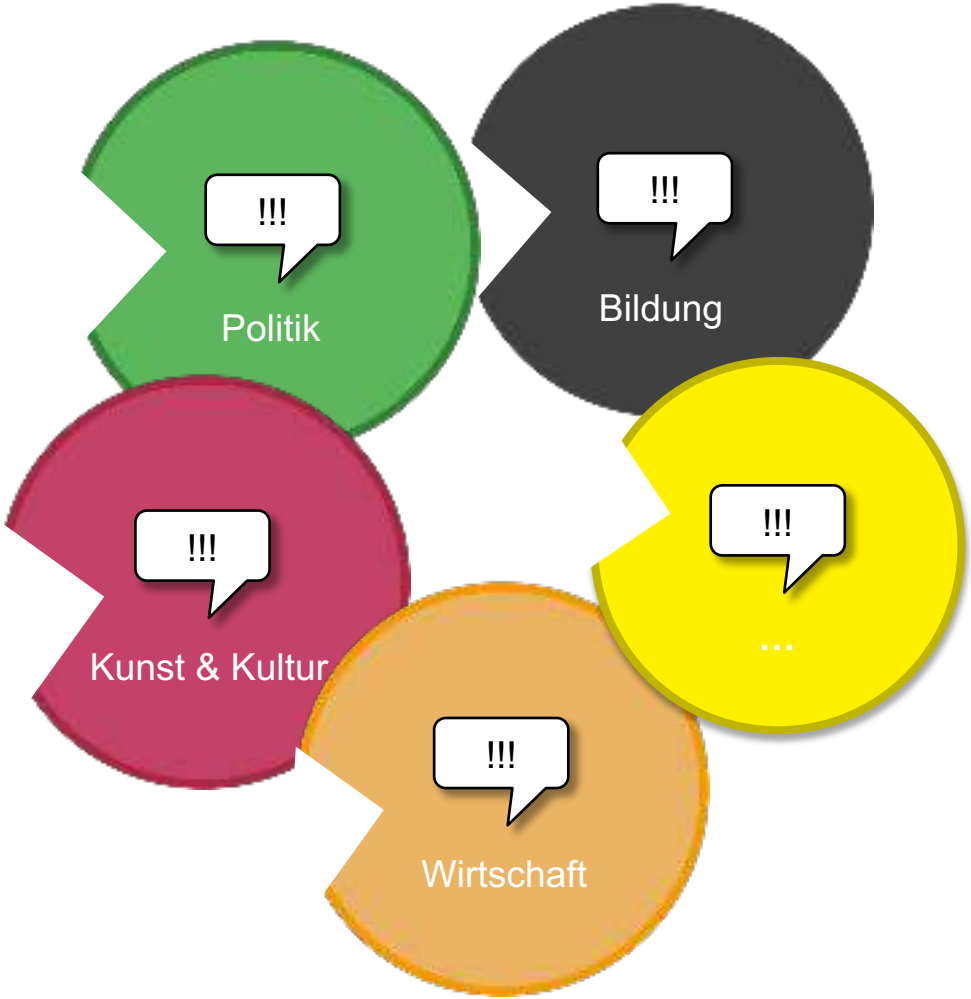
https://www.sans.org/security-awareness-training/reports/2018-security-awareness-report
https://www.sans.org/security-awareness-training/reports/2017-security-awareness-report

Was nun?


Bla bla bla
Security bla bla
Bla bla bla Firewall
bla bla
Bla bla bla
Verschlüsselung bla bla
Bla bla bla
Phishing bla bla
Bla bla bla
DNSSEC bla bla
Security Experten


???
Politik
???
Bildung
???
Kunst & Kultur
???
...
???
Wirtschaft


Bla bla bla Security bla bla
Bla bla bla Firewall bla bla
Bla bla bla Verschlüsselung bla bla
Bla bla bla Phishing bla bla
Bla bla bla DNSSEC bla bla
Security Experten


!!!
Politik
!!!
Bildung
!!!
Kunst & Kultur
!!!
...
!!!
Wirtschaft


INFORMATION
Ich chum
drus

Bohemian Browser Ballett
Live · The Page · February 1 · 🌍

Wir wünschen einen erfolgreichen Ändere-Dein-Passwort-Tag.

[redacted] Michael [redacted] Lustig, aber sachlich natürlich absolut falsch.
Denn auch wenn die Server gehackt werden, was im ganzen passiert, sind die Passwörter dort gehascht und dann muss man eben doch wieder raten (also nicht gehackt, gibt's hoffentlich ein neues DSGVO-Bußgeld) ... See More

3d

^ Hide 11 Replies

[redacted] David [redacted] Gehashes und vorher "salted", denn für die gängigen Hash-Algorithmen gibt es ja schon diverse Rainbowtables ...

3d

[redacted] Irene [redacted] Toll. Sehr verständlich. Um was genau geht's? Und was zur Hölle ist gehascht?

3d

[redacted] Michael [redacted] rene [redacted] hashen bedeutet mit einem mathematischen Einweg-Verfahren das Passwort unleserlich zu machen. Beispielsweise ist die Quersumme eine solche Möglichkeit.
Wenn deine PIN 123 ist, man aber nur die Quersumme (6) speichert, kann man damit nicht sagen, wie dein Passwort ist (kann ja auch 600, 222... sein). In der IT ist das natürlich deutlich komplexer. Damit verhindert man, dass eine Person das Klartextpasswort erfährt und sich damit versucht bei anderen Diensten einzuloggen.

Und bezüglich Salt, ja, wobei der eben auch nur wichtig ist, solange Personen Passwörter verwenden, die man erraten kann. Aber ja, nutzt Salt 😀

3d

[redacted] Daniel [redacted] r Aber was bringt das hashen wenn der Hacker dann weiß, welches Kriterium das Passwort erfüllen muss und einfach ein gleichwertiges Passwort nutzen könnte? (Frage von einem Laien)

2d

[redacted] Michael [redacted] Daniel [redacted]
Naja, wenn ich weiß wie der Hash ist, weiß ich (im Normalfall) dann eben nicht dein Passwort, welches du vielleicht woanders nutzt. Ich kann also, wenn ich hier die Daten deines Facebook-Accounts habe, eben noch lange nicht deinen Paypal-Account, deine E-Mailadresse oder ähnliches direkt übernehmen.

Ich bin mir nicht ganz sicher, ob das die Frage beantwortet, weil ich das „gleichwertige Passwort" nicht ganz verstehe. Falls es um mehrere Lösungen geht, die beim hashen richtig wären (wie beim Beispiel der Quersumme), dann gibt es diese beim hashen zwar theoretisch, aber praktisch dürfen diese nicht vorkommen.

2d

https://www.facebook.com/bohemianbrowserballett/
https://presse.funk.net/format/bohemian-browser-ballett/

1. “Security” in allgemeinen Diskurs einbringen
2. Öffnen, anpassen, ermöglichen
3. Anlaufstellen anbieten

Quellen

Slide 24:
https://www.com-magazin.de/news/sicherheit/faktor-mensch-in-cyber-security-1531813.html
https://www.computerworld.ch/security/veranstaltung/faktor-mensch-mitarbeiter-einfallstor-cyberkriminelle-1580533.html
https://creditreform-magazin.de/2018/10/04/mittelstandsbotschafter/joergasma/cyber-security-warum-der-faktor-mensch-so-wichtig-ist/
https://www.agendadigitale.eu/sicurezza/se-anche-chi-dovrebbe-proteggerci-diventa-una-vittima-chi-si-occupera-dellinsicurezza-della-pa-italiana/
https://www.cybersecurity360.it/cultura-cyber/il-fattore-umano-una-vulnerabilita-nei-processi-di-sicurezza-aziendale/
https://www.key4biz.it/il-fattore-umano-e-il-vero-problema-della-cybersecurity/219586/
https://www.techrepublic.com/article/why-the-human-factor-is-an-evergreen-problem-in-cybersecurity/
https://www.cso.com.au/article/647848/human-factor-driving-web-application-security-flaws/
http://globbsecurity.fr/facteur-humain-plus-gros-danger-cybersecurite-43421/
https://www.solutions-magazine.com/cybersecurite-investissez-facteur-humain/
https://www.datenschutz-praxis.de/fachnews/der-mensch-bleibt-schwachstelle-nr-1-bei-cybersecurity/

Slide 20:
https://www.swiss-isa.ch/
https://hacknowledge.com
https://www.isss.ch
https://www.melani.admin.ch/melani/de/home.html
https://www.digitale-gesellschaft.ch/
https://ictswitzerland.ch/
https://ebas.ch/en/
https://www.ccc-ch.ch/
http://www.swissict.ch/
https://www2.deloitte.com/
https://www.sig-switzerland.ch/
http://www.dxc.technology/
https://www.pwc.ch/de.html
https://www.ey.com/gl/en/services/advisory/ey-cybersecurity
https://www.infoguard.ch
https://www.ispin.ch/
https://www.swisscom.ch/de/privatkunden/sicherheit/internet-security.html
https://www.compass-security.com/

Slide 21
https://www.sans.org
https://www.blackhat.com/
https://www.first.org/
https://insomnihack.ch/
https://www.defcon.org/
https://www.rsaconference.com/
https://hack.lu/
https://bsideszh.ch/
https://www.swisscyberstorm.com/

SWITCH

Working for a better digital world

Katja Dörlemann
katja.doerlemann@switch.ch