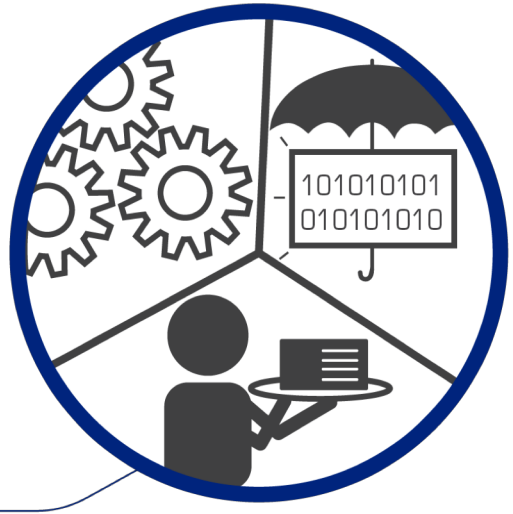
Security awareness & Escape Rooms – Behind the Scenes of HTH

SWITCH

Mathias Karlsson
mathias.karlsson@switch.ch

Riga, 2nd October 2019

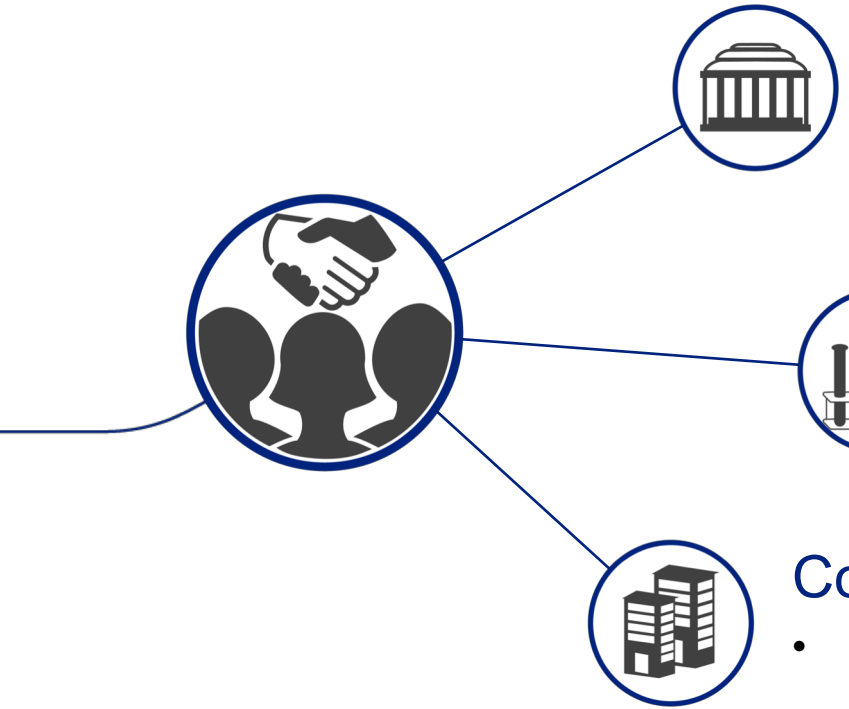
What we do



NREN (National Research and Education Network)

Registry for .ch/.li - cc TLDs

Our customers



SWITCH Community

- Swiss universities on tertiary level (academic sector) and their research institutions

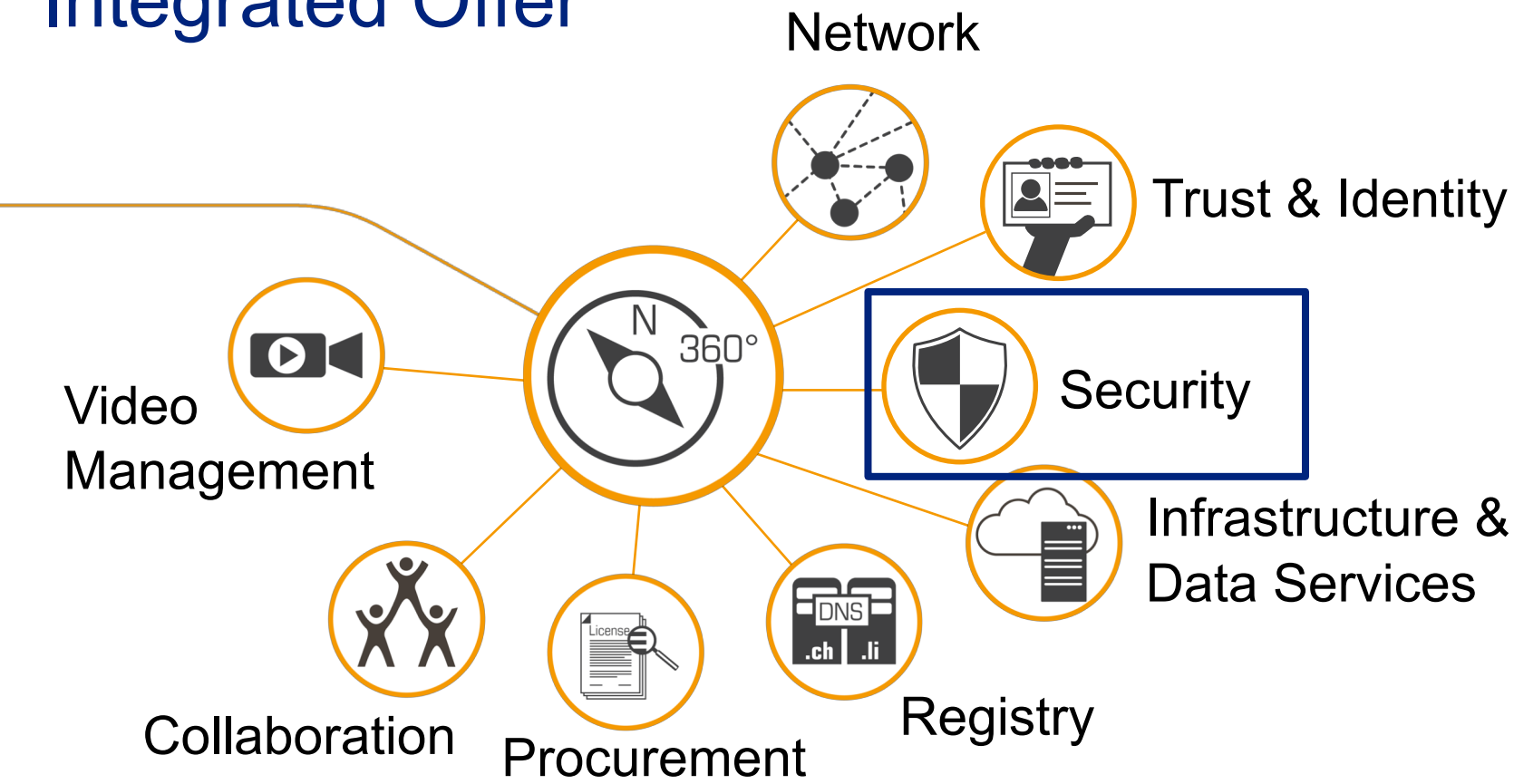
Extended community

- Other organizations involved in research or education

Commercial customers

- Registrars of .ch- and .li-Domain-Names, Swiss financial institutions, research-related industry and government

Integrated Offer



SWITCH-CERT

23 years SWITCH-CERT – information sharing and trusted community

Customers

- Universities
- Hospitals
- Banks

Services

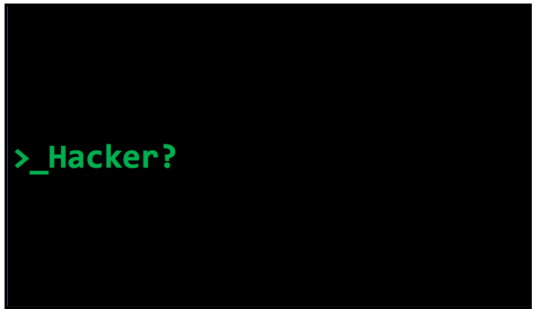
Cyber Threat Intelligence, Detection, Incident and Response as core competences

Your benefits

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

Hack The Hacker

Duration:	ca. 2 h
Number of participants:	max. 6 pers.
Target group:	employees of all fields, students
Location:	SWITCH Werdstrasse 2 8004 Zurich
Price:	on request


>_Hacker?


CYBER


SWITCH
I hacked a hacker
SWITCH
© 2018 SWITCH | 40

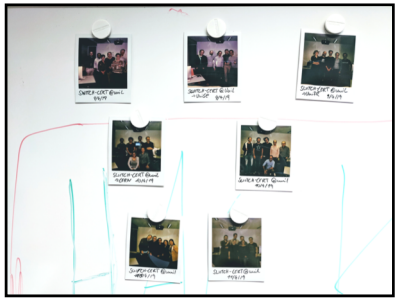
«Hack The Hacker» - Participants

Aprox. 350 participants
- since August 2018
- 50 Runs
- Part of onboarding

«Hack The Hacker» goes mobile

Frankfurt | Denic | Dec 2018

Lausanne | UniL | Apr 2019



Düsseldorf | Phishbot | Jun 2019

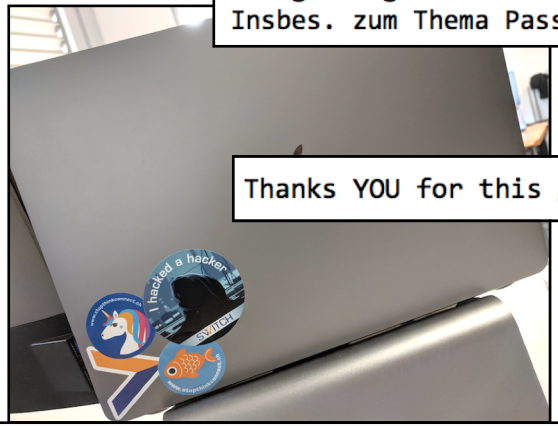
Lugano | USI | Jul 2019

«Hack The Hacker» - Feedback

uns gehts gut. Wir hatten im Nachgang noch viele positive Rückmeldungen. Insbes. zum Thema Passwort-Management.

Danke für das tolle Training!

Thanks YOU for this great hacking moment! It was indeed a lot of fun!

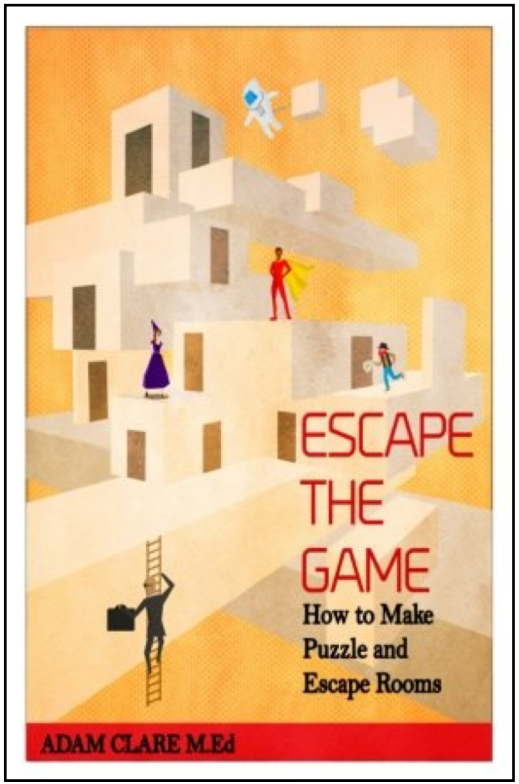


I'm happy about the feedback I received from my colleagues. It's an experience to redo :-)

War durchaus spannend, auch wie die Thematik bei nicht IT-iler ankam😊

Grazie mille per l'organizzazione e per l'opportunità.
Personalmente l'ho trovata un'esperienza molto ben strutturata, organizzata e formativa. I due responsabili sono stati chiari, esaurienti nelle spiegazioni e anche molto disponibili.

gather information



Escape The Game

How to Make Puzzle and Escape Rooms

Adam Clare

CreateSpace Independent Publishing Platform 2016

put a team together

Oli: IT security, games, escape rooms

Jakob: IT security, music

Andreas: IT security, business

Antoine: IT security, programing

Livia: communications, marketing

Katja: security awareness, communications

Tips:
- multidisciplinarity!
- team skill set determines possibilities
- enthusiasm values as much as skills!

attune the team

have a workshop

1. Security Awareness using an Escape Room
   a. objective
   b. to keep in mind
   c. awareness topics

2. Our Escape Room
   a. theme & topic
   b. setting
   c. storyline
   d. puzzles
   e. additional stuff

1. a. – objective

- raising interest for security
  - positive contact with IT security
  - demystify hackers
  - get rid of reservations

- reflect knowledge about IT security
  - apply knowledge
  - review knowledge
  - improve knowledge

1.b. – to keep in mind

- use existing resources
  - SWITCH skills, rooms, devices etc.

- set up has to be flexible
  - showroom at SWITCH
  - assemble and dismantle
  - transportable

- fun for everybody
  - tech-experts
  - other-experts

- duration: max. 1h

1.c. – awareness topics

- phishing
- social engineering
- dumpster diving
- data backup
- get help from experts
- encryption
- password security
- install updates
- malware / virus
- USB drives

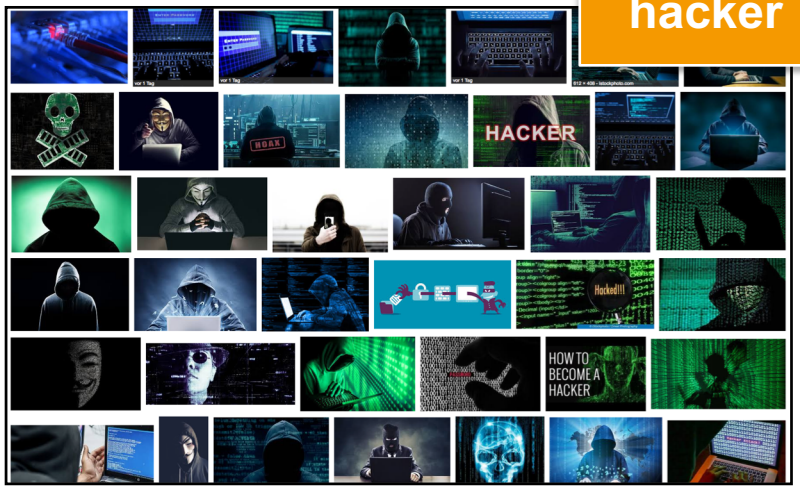
2.a. – theme & topics

2.b. – setting

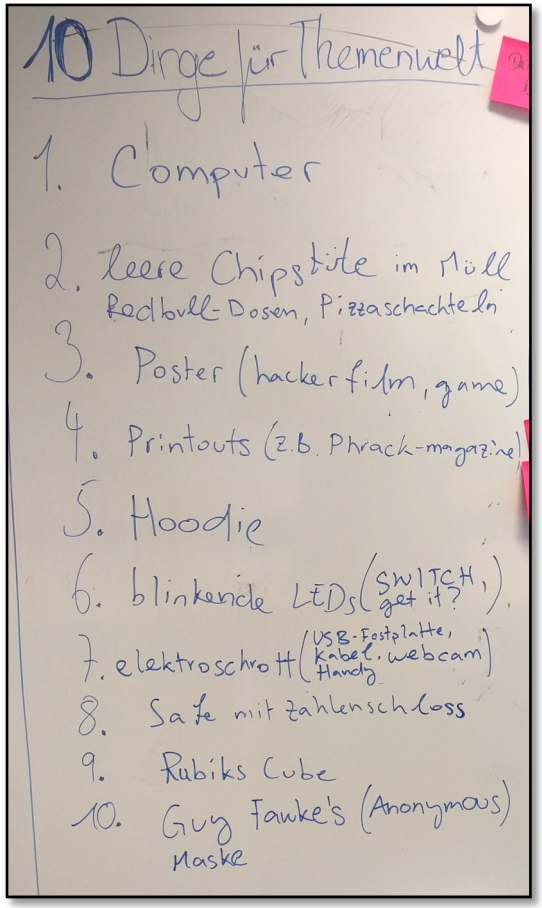
10 must haves for creating a “hacker” atmosphere

cyber crime

hacker



ransomware



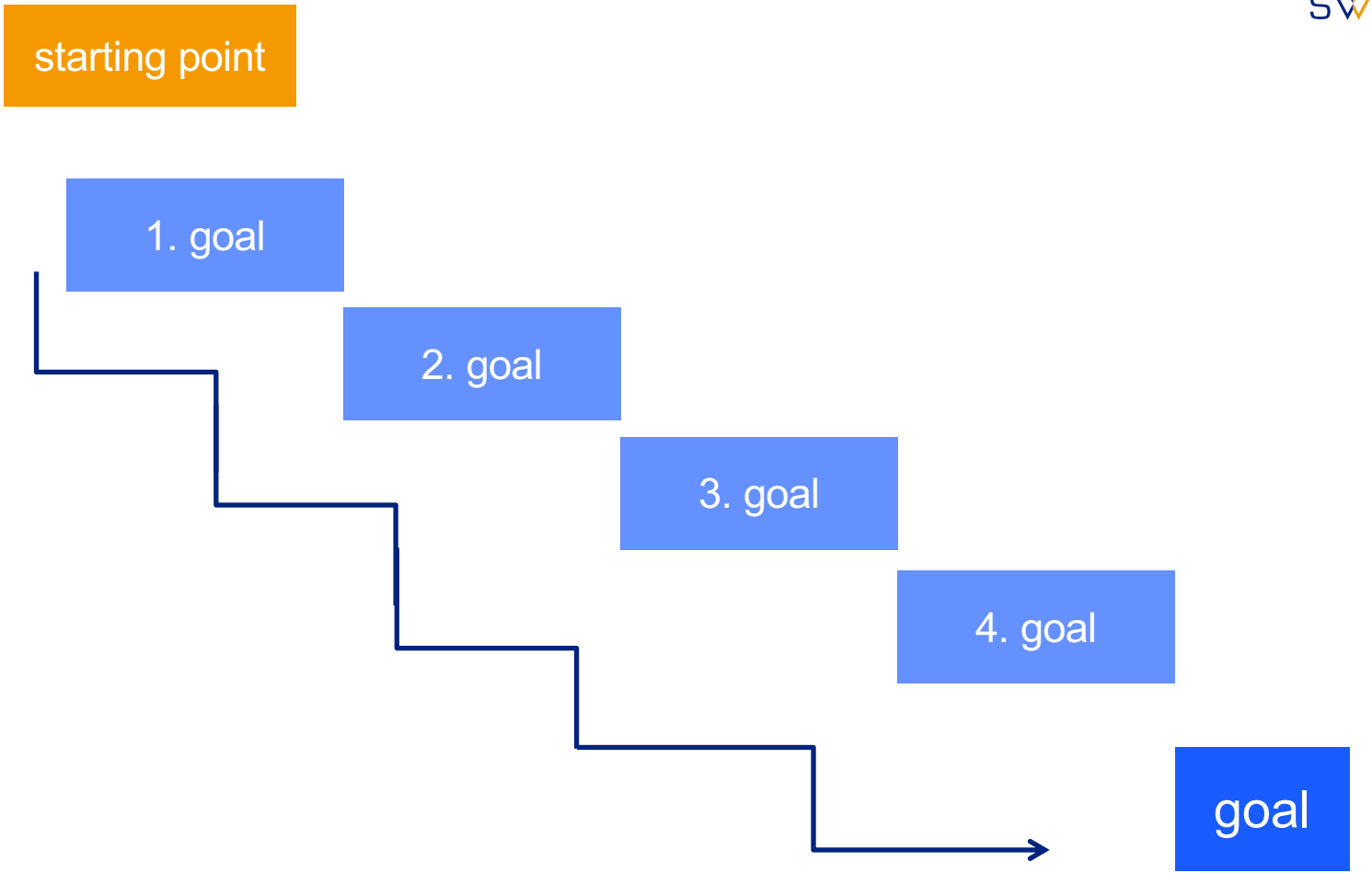
1. Computer
2. Trash: empty chips bag, Red Bull, pizza delivery box
3. Posters: Hacker movie, game
4. Printouts, i.e. Phrack magazine
5. Hoodie
6. Blinking LEDs
7. Electronics plunder: USB disk, cables, webcam, devices
8. Safe, PIN code
9. Rubiks Cube
10. Guy Fawk's mask

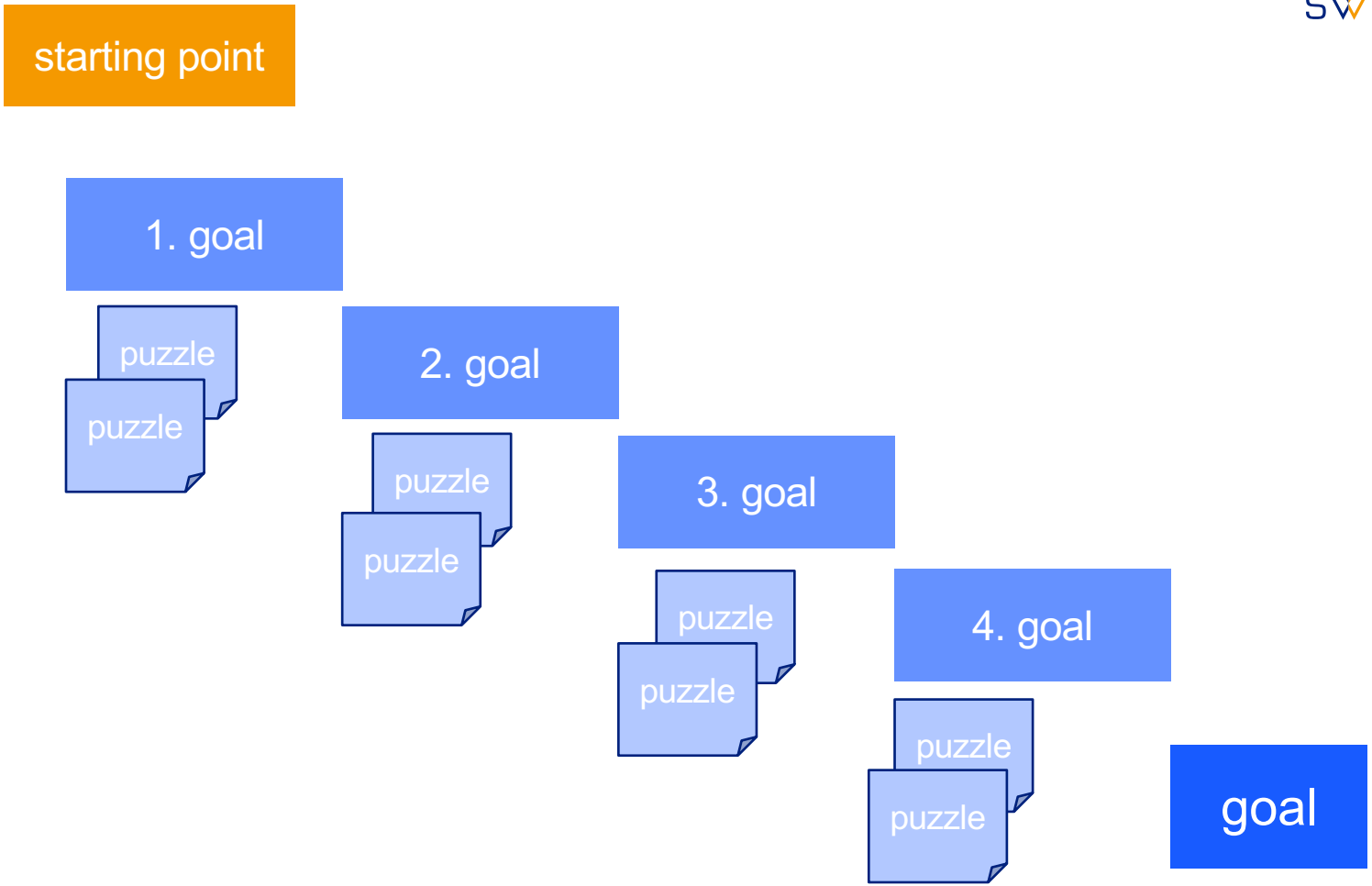
2.c. – storyline

reaching the goal step by step

starting point

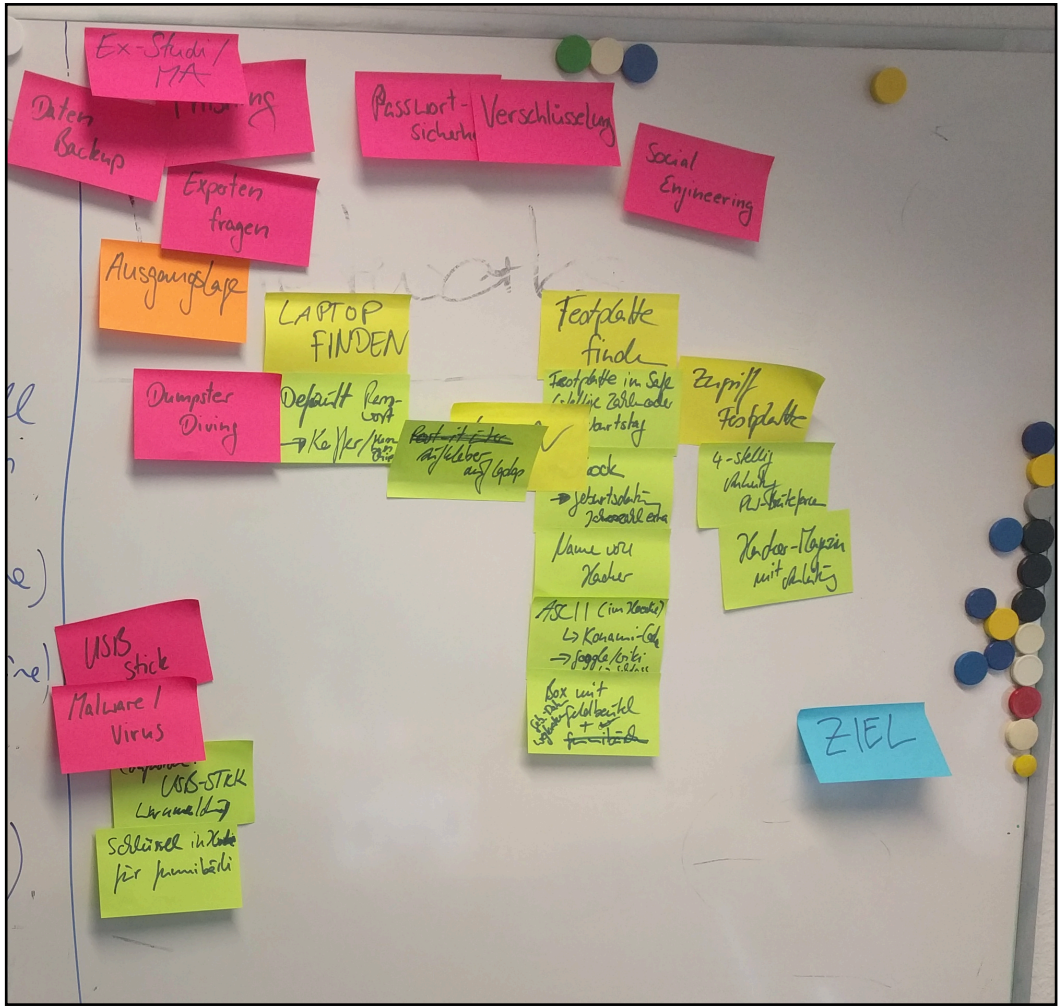
goal


starting point
1. goal
2. goal
3. goal
4. goal
goal


starting point
1. goal
puzzle
puzzle
2. goal
puzzle
puzzle
3. goal
puzzle
puzzle
4. goal
puzzle
puzzle
goal

puzzle types

- **logical puzzles**
  search for patterns/schemes, similarities
- **codes, crypto**
  encrypted text, numerical code
- **puzzle combination**
  solution of puzzle A is needed to solve puzzle B
- **maze, scouts**
  follow hidden signs etc.
- **teamwork**
  One person reads the manual, the others execute
- **hidden hints**
  Hide hints


Ex-Studi / MA
Daten Backup
Passwort-Sicherh
Verschlüsselung
Social Engineering
Exoten fragen
Ausgangslage
LAPTOP FINDEN
Dumpster Diving
Default
Textplatte finde
Zugriff Textplatte
4-stellig
USB Stick
Malware / Virus
USB-Stick
ZIEL

2.e. – additional stuff

provide information and spread the news

2.e. – additional stuff

- name
- moderator/host
- website:
  - introduction
  - pictures of participants
  - additional information on awareness topics
  - contact
- flyer
- sticker

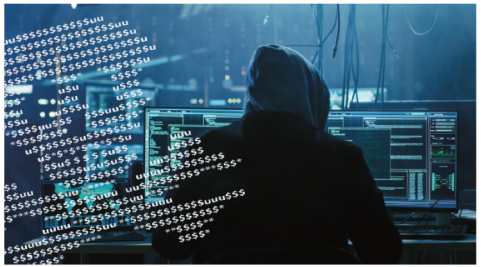
2.e. – additional stuff

- name: Hack The Hacker
- moderator/host: team of 2 (Tech/Non-Tech)
- website: https://swit.ch/hack-the-hacker
  - introduction
  - ~~pictures of participants~~
  - additional information on awareness topics
  - contact
- flyer
- sticker

Tips:
- avoid “Security” in title
- tip flyer gives a good feeling
- team picture boosts the team spirit

Hack the Hacker

Das SWITCH Security Awareness-Erlebnis



SWITCH

SWITCH-CERT – ein führendes nationales Kompetenzzentrum

SWITCH-CERT schützt gegenwärtig Mitglieder der wissenschaftlichen Gemeinschaft in der Schweiz, Inhaber von .ch- und .li-Domains, Schweizer Banken und naturgemäss die gesamte Schweizer Internetgemeinde.

SWITCH betreibt das Schweizer Forschungs- und Bildungsnetzwerk, ein Backbone mit über einer Viertelmillion aktiven Geräten, sowie die DNS-Infrastruktur (Domain Name System) für .ch und .li. Unternehmen der Schweizer Finanzbranche erhalten zudem Unterstützung bei der Bekämpfung von Angriffen auf ihre IT-Assets.

Diese einzigartige Kombination von Aktivitäten verschafft SWITCH-CERT, dem Computer Emergency Response Team von SWITCH, einen Vorsprung beim Schutz seiner Kunden. Dank seinem Expertenwissen und seinem weitreichenden internationalen Partnernetzwerk kann es handeln, bevor Probleme eskalieren.

SWITCH
P.O. Box, CH-8021 Zurich
Phone +41 44 268 15 40
cert@switch.ch
https://www.switch.ch/security

«Hack The Hacker» - Los geht's!

Ein falscher Klick und schon ist es passiert: Ein bösartiger Hacker hat das Computersystem Ihrer Organisation mit Ransomware infiziert. Alle Daten Ihrer Organisation sind verschlüsselt und nicht mehr verfügbar – eine Katastrophe! Was nun?

Ihr Team ist auserwählt, den Hacker zu überlisten und die Daten zurückzuholen. Das Schicksal der gesamten Organisation liegt in Ihren Händen!

Finden Sie den Code zur Entschlüsselung der Daten?

WannaCry
Seit 2017 aktiv, verbreitet sich über andere befallene Computer im gleichen Netzwerk

Petya
Seit 2016 aktiv, verbreitet sich via E-Mail (häufig als Bewerbungsschreiben getarnt)

Locky
Seit 2016 aktiv, verbreitet sich via SPAM-Mails

Was ist Ransomware?

Ransomware ist Schadsoftware, die alle Daten auf Ihrem Computer verschlüsselt. Ohne den korrekten Entschlüsselungs-Code sind all Ihre Dateien verloren. Der Angreifende erpresst Sie, indem er Ihnen gegen Bezahlung den Code anbietet.

Weltweit wurden zwischen April 2016 bis März 2017 mehr als 2,5 Mio. Nutzer mit Ransomware konfrontiert. 2017 war jedes zweite Unternehmen von Ransomware betroffen. Der durchschnittliche Schaden pro Fall belief sich dabei auf ca. CHF 123'000.

STOP.THINK.CONNECT.

Nützliche Informationen zu Security-Themen finden Sie auf:
https://www.stopthinkconnect.ch.

SWITCH

Security zum Anfassen

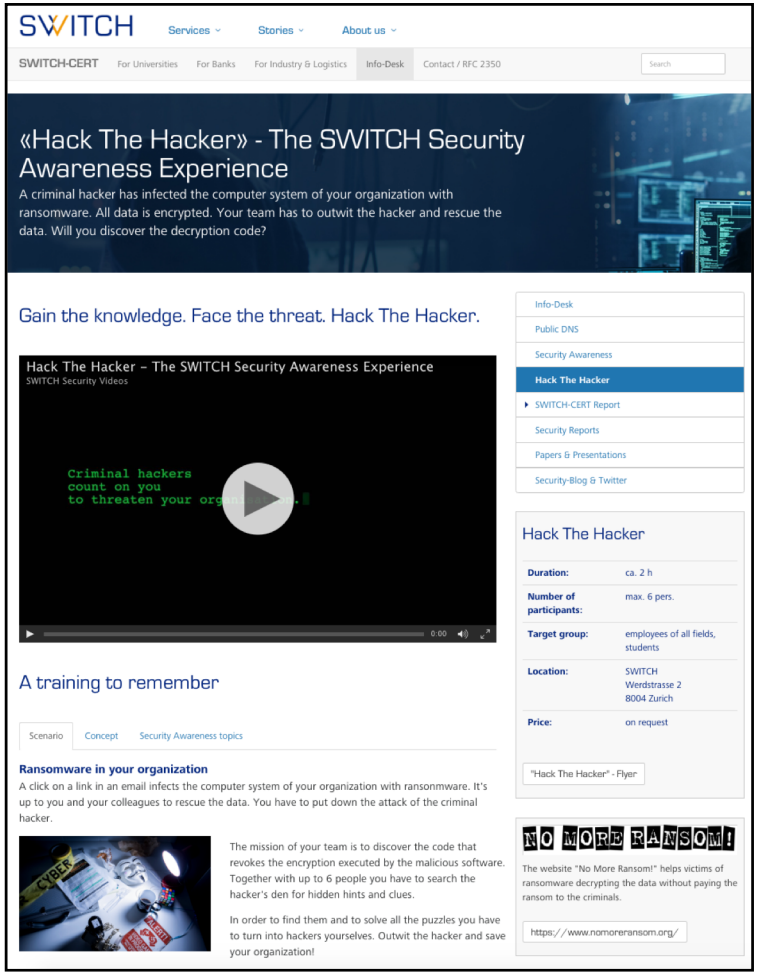
«Hack The Hacker» - das SWITCH Security Awareness-Erlebnis bietet Security zum Anfassen. Als Team müssen die Teilnehmenden die Daten Ihrer Organisation vor der Ransomware-Attacke eines kriminellen Hackers retten. Einführend wird Basiswissen über Security vermittelt, das dann im spielerischen Rahmen praktisch angewendet werden muss. Abschliessend wird das Gelernte und Erlebte in einem Debriefing wiederholt und diskutiert.

Security Awareness-Themen:
- Phishing
- BackUp
- Dumpster Diving
- Brute-Force-Methode
- Social Engineering
- Passwortsicherheit
- Encryption

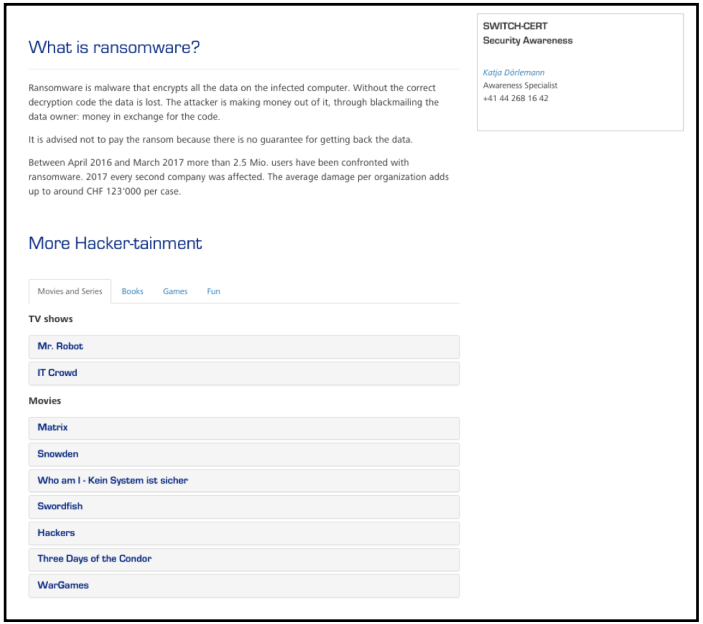
Ein unvergessliches Training

«Hack The Hacker» ist Security-Training mit Spass und nachhaltigem Erfolg. Durch den Mix aus Theorie und Praxis, Fiktion und Realitätsbezug sowie die Bewältigung der Aufgabe als Team bleibt das Erlebte in Erinnerung und motiviert zur weiterführenden Auseinandersetzung mit dem Thema.

Dauer	ca. 2 Stunden
Teilnehmerzahl	max. 6 Personen
Veranstaltungsort	SWITCH Werdstrasse 2 8004 Zürich
Kontakt	Katja Dörlemann katja.doerlemann@switch.ch +41 44 268 16 42
Website	https://swit.ch/hack-the-hacker
Zielgruppe	IT-Mitarbeitende, Mitarbeitende aller Bereiche, Studierende
Preis	auf Anfrage



https://swit.ch/hack-the-hacker




CYBER
CYBER
CYBER
CYBER
CYBER
CYBER
CYBER

go shopping

Transport-Koffer
Polaroid plus Film
Hacker Laptop
Victim Laptop
Baby Phone/Kamera
Safe
Poster
LEDs
Festplatte
Funkgeräte
Alukoffer
Bücher
Raspberry Pi
Rasperry Pi Zubehör
Lautsprecher
Rubiks Cube
Hoodie
USB Stick
Steckerleiste
Adapter
Schreibtischlampe
Box + Kette
Mouse
Schloss (Master Lock)
Laptop-Sticker
Cyber Absperrband und Aufkleber
alte T-Shirts/Hosen/Schuhe
Geldbeutel
Postits, Schreiber, Schere, Klebeband
UV-Neon Stift
Gummibärchen
Kasse
Maske
Pizzaschachteln
"Müll"
ASCII-Tabelle
Hacker Polaroid
Ausweise
Anleitungen/Artikel
Sticker Rubiks Cube
Batterien
Safe Dose

find location and decorate

test, adapt, document

Escape Room für SWITCHIES

Freitag, 07. September 2018 Jakob Dhondt

Hoi Zäme!

Damit jeder einmal den bösen Hacker überlisten kann, haben wir
den Escape Room selbst einmal erleben kann. Pro Termin können
euch bei Interesse einfach in folgendes Doodle ein! https://doodl

Und unbedingt den Trailer anschauen!

Liebe Grüsse,

Euer Escape Room Team

Durchlauf checklisten

Checkliste Materialvorbereitung am Vortag

- Sicherstellen, dass die Funkgeräte funktionieren und die Batterien genügend geladen sind
- Babycam aufladen bzw. sicherstellen, dass das Ladegerät verfügbar ist

Checkliste Raum einrichten (vor jedem Durchlauf)

- "Alert"-Schild aussen über Raumbezeichnung "Marketing" hängen
- Hacker Laptop/Koffer
  - Laptop resetten
    - Laptop einschalten, sobald das Thinkpad-Logo verschwindet, `Shift` gedrückt halten. Es erscheint ein Boot-Menü
    - Option "Clonezilla Restore Image" mit dem Pfeiltasten auswählen und `Enter` drücken
    - Username `grub` eingeben, `Enter` drücken
    - Passwort `czberczber` eintippen (eigentlich `cybercyber`, aber aufgrund entlischer Tastatur ist `y=z`)
    - Frage `are you sure you want to continue?` mit `z` beantworten und Enter drücken. (Wieder `y=z` wegen Englischer Tastatur)
    - Der Prozess dauert ca. 5 Min.; das Gerät schaltet sich selber aus
  - Laptop in den Koffer packen
  - Stromkabel/Ladegerät in den Koffer packen
  - Maus in den Koffer
  - UV-Lampe in den Koffer
  - Koffer schliessen, zufällige Zahlencodes ohne Nullen einstellen
- Konami-Rätsel:
  - Ausweise in die Brieftasche
  - Brieftasche in die Kiste
  - Kiste mit Kette und Konami-Schloss verschliessen. Kette muss fest angezogen sein.
  - Konami-Schloss zwei mal drücken zum resetten.
  - Zettel mit Konami-Zahlencode zwischen die Bücher im Regal, so dass er leicht herausragt.
  - Kette herunterhängen lassen, so dass sie in der Nähe des Zettels hängt
- Hash crack-Rätsel
  - Festplatte in den Safe, Safe verschliessen
  - Schranktür zum Safe zu ziehen
  - Zettel mit Hash in die leere, rote Kasse
  - Münzenfach einlegen, Gummibärchen dazugeben
  - Kasse verschliessen
  - Kassenschlüssel in die Rechte Hoodie-Tasche
  - Hoodie über den Schreibtischstuhl hängen
  - Hash crack-Anleitung sichtbar mit den anderen Artikeln auf dem Schreibtisch platzieren
- Sonstige Kleinigkeiten
  - Ironman-USB-Stick an die Stehlampe hängen
  - Spoiler Material der vorangegangen Teilnehmergruppe entfernen (z.B. beschriebene Post-its, auch auf Durchdruck auf die darunterliegenden Post-its
- Raum "starten"
  - Steckerleiste am Eingang einstecken
  - Normales Deckenlicht ausschalten
  - Nach ca. 30 sekunden sollten die LEDs leuchten
  - Nach ca. 40 Sekunden sollte Musik laufen, ggf. Lautstärke an den Boxen anpassen (Musik hörbar, aber nicht laut, so dass man normal sprechen kann
  - Türe von aussen schliessen

Briefing - Vorbereitung

- Victim-Laptop resetten:
  - Laptop starten

Wenn es los geht / Tipp management

- **Wichtig:** Die Spielleiter MÜSSEN sicherstellen, dass die Teilneh
- **Spielszenario:** Die Spielleitung sind Experten aus dem SWITCH-
  - CERT und Helfer arbeiten gleichzeitig an der Entschlüsselun
  - Die Experten unterstützen die Helfer aus dem CERT heraus
- 60-min-Timer starten, wenn die Ransomware von den Teilnehmen
- Nicht vergessen: Im Spielszenario gibt es keinen Sichtkontakt, d.h.
  - "Was habt Ihr bisher herausgefunden?"
  - "Habt Ihr den Laptop vom Hacker gefunden?"
  - "Woran arbeitet Ihr gerade?"
  - "Braucht Ihr Hilfe?"
- **T-50 min:** Koffer offen
  - Tipp: "Eine bekannte Taktik unter Hackern ist 'Dumpster diving', d.h. das Durchsuchen von Müll nach wertvollen Informationen"
  - Tipp: "Sieht der Koffer neu aus? Manche Menschen sind faul und ändern Passwörter gar nie"
- **T-40 min: Laptop login**
  - Tipp: "Passwörter oder Hinweise darauf befinden sich meist auf dem Gerät selber oder in ummittelbarer Nähe"
  - Tipp: "Habt Ihr den Koffer gründlich durchsucht?"
  - Tipp: "Wir haben gerade herausgefunden, dass der Hacker einer Gruppierung namens Internet Society zugehörig ist"
- **T-25 min und T-10 min:** Entweder Safe offen und Festplatte gefunden oder Hash gecrackt, ansonsten Tipps zu einem der beiden Rätsel geben. Jenachdem, welches gerade in Bearbeitung ist :
  - **Safe-Rätsel:** Konami code -> Brieftasche gefunden -> Safecode
    - Tipp: "Bücherregale werden gern als Versteck verwendet"
    - Tipp: "Zahlen auf dem Zettel? Könnte ein Code sein? Vielleicht findet sich im Raum ja ein Hinweis, wie man diese Zahlen umwandeln könnte"
    - Tipp: "Konami-Code? Hm, sagt uns auch nichts. Aber schaut doch mal im Internet nach"
    - Tipp: "Viele persönliche Informationen findet man im Internet, z.B. auf Social Media"
  - **Hash-Crack-Rätsel:** Schlüssel gefunden -> Kasse geöffnet -> Hash cracked (mit Anleitung)
    - Tipp: "Habt ihr alles durchsucht? Kleidungsstücke etc." -> Schlüssel zur Kasse
    - Tipp: "Für das Cracken von Hashes gibt es Hilfsprogramme. Vielleicht findet sich ja irgendwo eine Anleitung?"
    - Tipp: "Ein richtiger Hacker muss auch mal die Konsole bedienen"
- **T-5 min:** Beide Rätsel sollten nun gelöst sein, sonst Tipps zu beiden Rätseln
- **Ende:** Beendet ist das Spiel erst, wenn die Teilnehmenden erfolgreich waren. Sollten die Teilnehmenden den Code nach 60 min nicht gefunden haben, geht das Spiel weiter

Tips:

- no end of game by end of time
- tip management has to support a feeling of success
- positive encouragement no matter what

4 learnings

1 Development is one thing, maintaining the other:

When? Who? How long? How many? Time to reset?

2 What can break, will break:

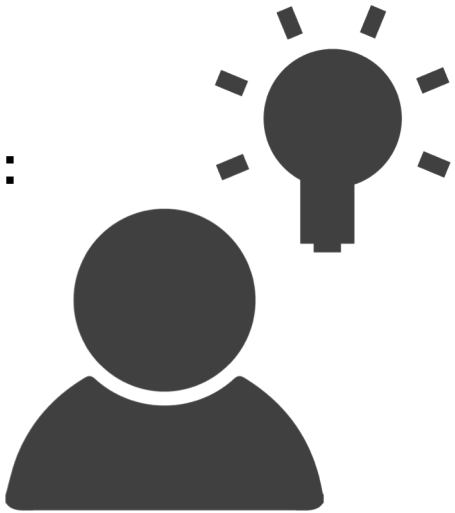
material stock, include in budget (Rubik's Cube!)

3 For some it's a fun training, for others it's just fun:

know your target group and manage expectations

4 Sweets prevent frustration:

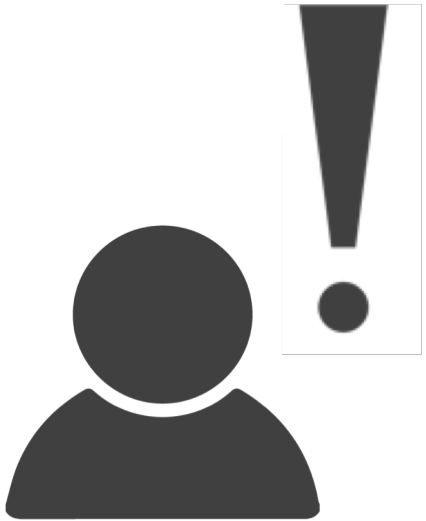
feeling of success and "dead end-flag"



1. a. – objective

- raising interest for security
  - positive contact with IT security
  - demystify hackers
  - get rid of reservations

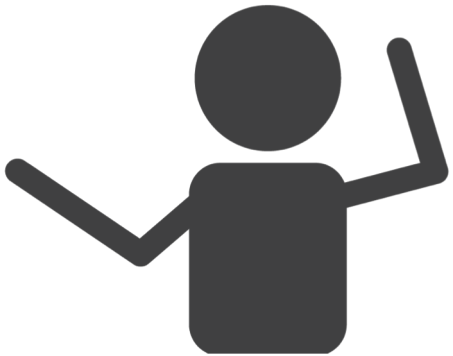
- reflect knowledge about IT security
  - apply knowledge
  - review knowledge
  - improve knowledge



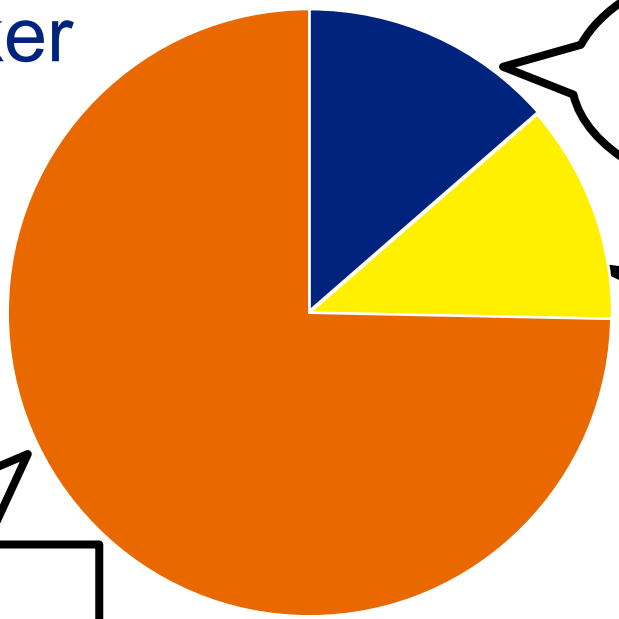
AWARENESS
Increase awareness and interest in a specific topic

EDUCATION
Teaching new skills and the theory behind them

TRAINING
Teaching and practicing (new) skills



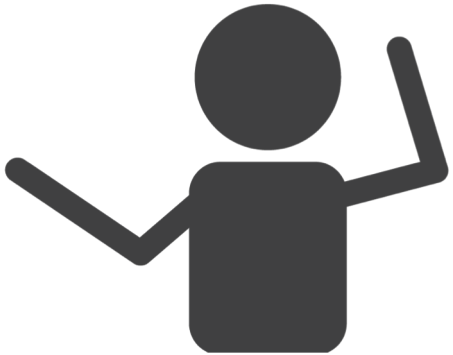
Hack The Hacker



EDUCATION
Teaching new skills and the theory behind them

TRAINING
Teaching and practicing (new) skills

AWARENESS
Increase awareness and interest in a specific topic



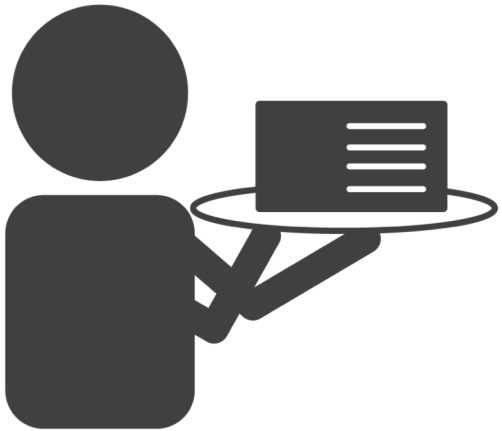
What security awareness escape rooms can do:

- raise interest in security
- empower participants to deal with IT related issues
- improve the reputation of your organization
- improve teamwork

What security awareness escape rooms can**not** do:

- provide sustainable knowledge about IT security
- educate a large amount of employees at a good price
- turn into education at a good price
- adapt to new topics quickly

Hack The Hacker
Train The Trainer concept



SWITCH

Working for a better digital world

Katja Dörlemann
katja.doerlemann@switch.ch