Introduction to IT Security for Data Scientists

SWITCH

matthias.seitz@switch.ch
daniel.weber@switch.ch

Bern, 13th of June 2019

Schedule

09:15 Welcome
09:30 Lecture
10:30 Coffee break
11:00 Lecture
12:30 Lunch break
13:30 Lecture
15:00 Coffee break
15:30 Lecture
17:00 End

Who are we?

- Matthias Seitz
  - 15+ years of experience in IT security
  - BSc Computer Science
  - Currently IT Security Engineer / Product Manager @SWITCH

- Daniel Weber
  - 18+ years of experience in IT
  - BSc Computer Science
  - Currently IT System Administrator / Security Engineer @SWITCH

Mission

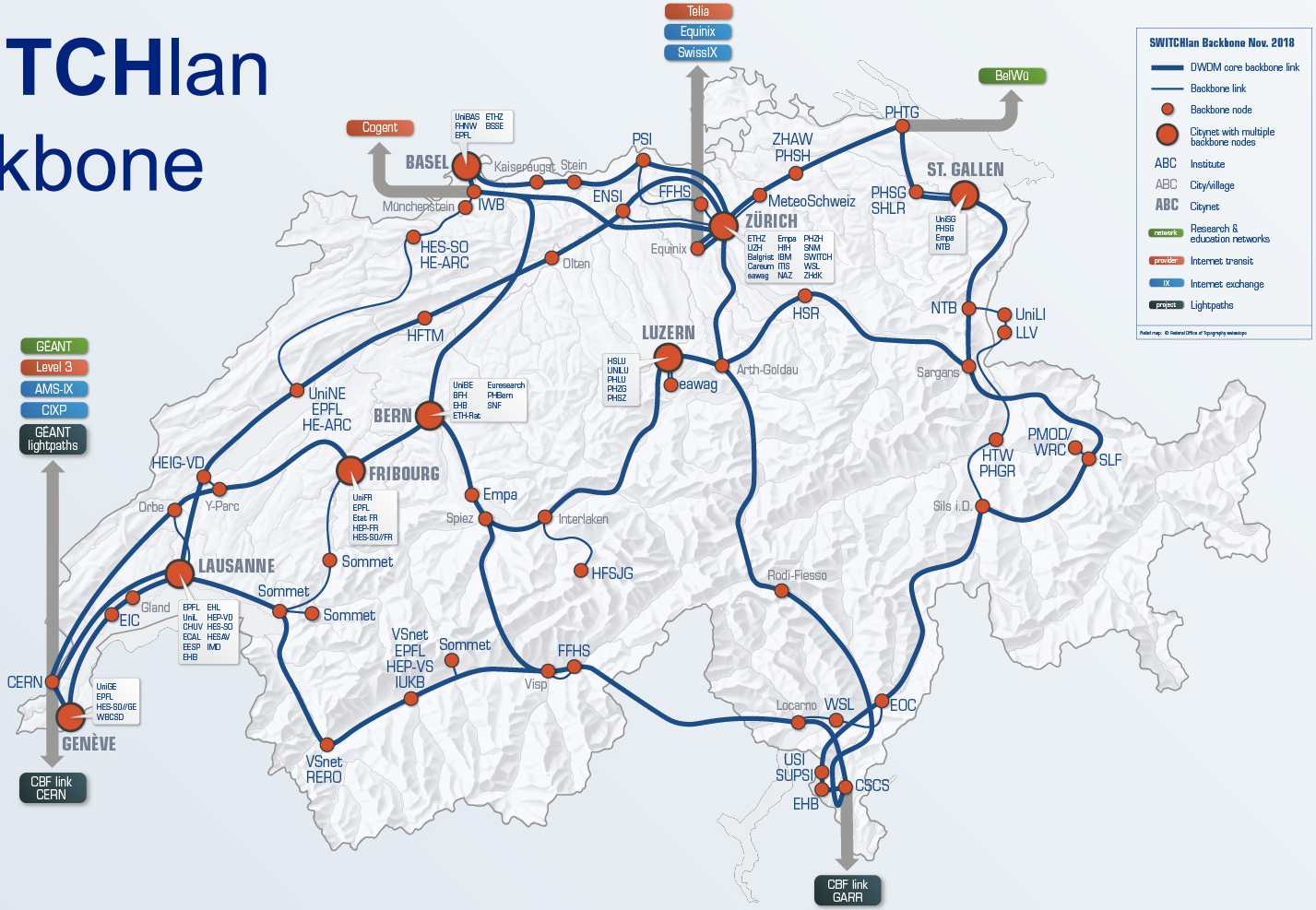
SWITCH is an **integral part of the Swiss academic community**.

Based on our **core competencies**

- Network
- Security
- Identity Management

SWITCH offers collaboratively developed ICT solutions that empower users in and beyond the academic world to achieve leading edge results in a globally competitive environment.

SWITCHlan Backbone



Registry

Your added value

Information sharing and trusted community

- Leading CERT/CSIRT in Switzerland
- National center of competence since 20 years
- Excellent national and international network
- Threat Intelligence from its own network

- Direct link to 14 experienced experts
- Successful cooperation with highest confidentiality level
- Neutral position as foundation for the Swiss universities

Our customers

Higher education

- Cantonal universities
- ETH domain with research institutions
- Universities of applied sciences
- Universities of teacher education

University-related organizations and administration

- Hospitals
- Pharmaceutical research

Commercial customers

- Retail banks
- Cantonal banks and regional banks
- Private banks
- Major banks

Our offer

20 years SWITCH-CERT – information sharing and trusted community

- Computer Security Incident Response
- Network Security Monitoring
- Trusted Collaboration Services
- Malware Monitoring & Analysis
- Malicious Domain Takedown
- Information & Awareness Services
- DNS Firewall Service

Security

20 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

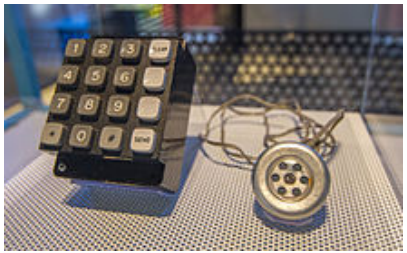
Comprehensive incident support and optimal network security, especially for the Swiss Internet

What are your expectations?

- What is your background?
- Who has already made experience with IT security?
- Are there already questions you ever wanted to ask about IT Security?

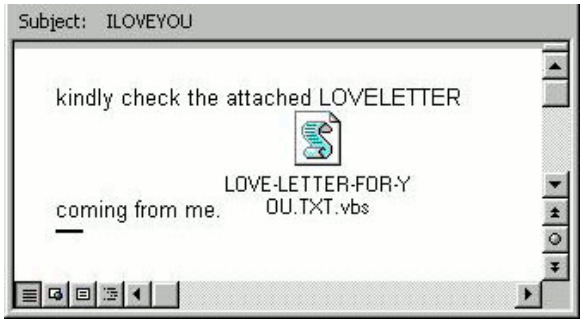
Everything has a beginning…

Everywhere Terminals
Accessible via Phoneline



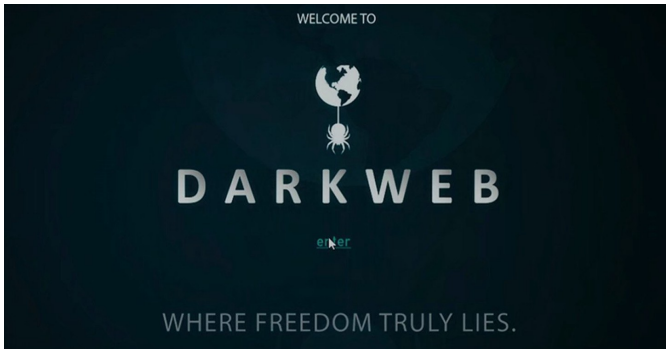
Phreaking
Phone and Freak

Computer Worms
Spread through the Internet



Tor and the Darkweb

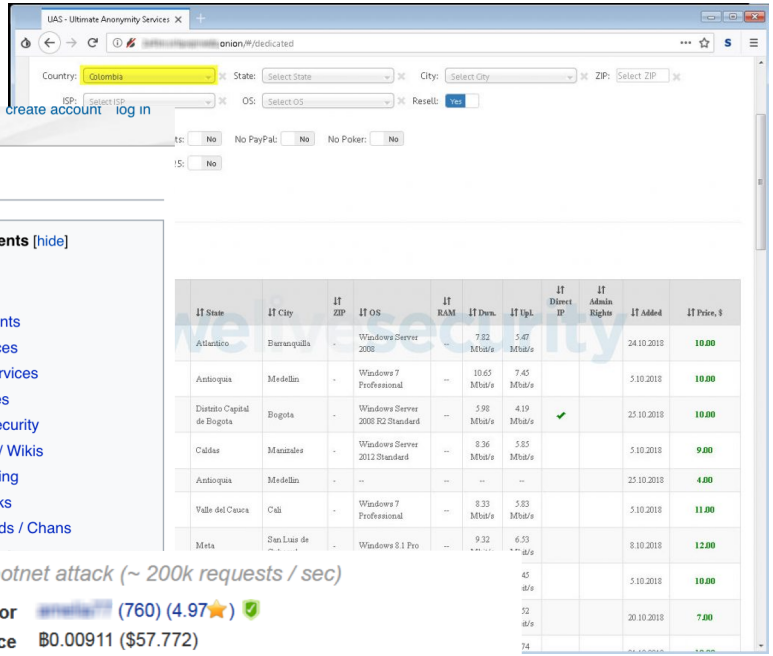
A Market evolved with Tor



Cyber Crime vs. Top 5 Fortune 500

Organization	Annual Revenue
Cybercrime	$1’500’000’000’000
Walmart	$500’343’000’000
Exxon Mobil	$244’363’000’000
Berkshire Hathaway	$242’137’000’000
Apple	$229’234’000’000
UnitedHealth Group	$201’159’000’000

Darkweb 5 min. search



main page | discussion | view source | history

The Hidden Wiki

Main Page

Welcome to The Hidden Wiki New hidden wiki url 2019

Add it to bookmarks and spread it!!!!

Editor's picks

Pick a random page from the article index and replace one of these slots with it:

1. The Matrix - Very nice to read.
2. How to Exit the Matrix - Learn how to Protect yourself and your rights, online and off.
3. Verifying PGP signatures - A short and simple how-to guide.
4. In Praise Of Hawala - Anonymous informal value transfer system.
5. Terrific Strategies To Apply A Social media Marketing Approach - Great tips for the internet marketer.

Volunteer

navigation
- Main page
- Recent changes
- Random page
- Rules of the site

search
Search The Hidden W
Go | Search

tools

Contents [hide]

1 Editor's picks
2 Volunteer
3 Introduction Points
4 Financial Services
5 Commercial Services
6 Domain Services
7 Anonymity & Security
8 Blogs / Essays / Wikis
9 Email / Messaging
10 Social Networks
11 Forums / Boards / Chans

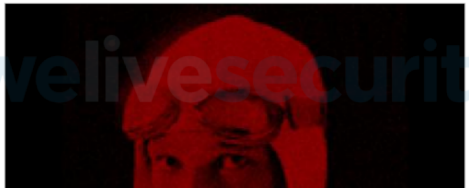
250g - 250kg 90% Pure Bolivian Flake Cocaine

Pure flake cocaine, high purity cocaine Fresh from across the border,that will bring you back to the old days. This coke is straight from the source. Pure, uncut & untouched. Off White with that shiny fish scale sparkle so you can guarantee purity Great for making free base and crack. Mostly rocks. The larger the order, the easier it is to receive just rocks. Multi-kilo shipments always receive full bricks. For Stealth and packaging related questions please firstly read our about section

State	City	ZIP	OS	RAM	Dwn.	Upl.	Direct IP	Admin Rights	Added	Price, $
Atlantico	Barranquilla	-	Windows Server 2008	--	7.82 Mbit/s	5.47 Mbit/s			24.10.2018	10.00
Antioquia	Medellin	-	Windows 7 Professional	--	10.65 Mbit/s	7.45 Mbit/s			5.10.2018	10.00
Distrito Capital de Bogota	Bogota	-	Windows Server 2008 R2 Standard	--	5.98 Mbit/s	4.19 Mbit/s	✔		25.10.2018	10.00
Caldas	Manizales	-	Windows Server 2012 Standard	--	8.36 Mbit/s	5.85 Mbit/s			5.10.2018	9.00
Antioquia	Medellin	-	--	--	--	--			25.10.2018	4.00
Valle del Cauca	Cali	-	Windows 7 Professional	--	8.33 Mbit/s	5.83 Mbit/s			5.10.2018	11.00
Meta	San Luis de	-	Windows 8.1 Pro	--	9.32	6.53			8.10.2018	12.00
						45			5.10.2018	10.00
						52			20.10.2018	7.00
						74				

3 hours ddos botnet attack (~ 200k requests / sec)

Vendor	[redacted] (760) (4.97★)
Price	Ƀ0.00911 ($57.772)
Ships to	Worldwide, Worldwide
Ships from	Worldwide
Escrow	No



Introduction to Information Security

The term “information security” means **protecting information and information systems** from **unauthorized access, use, disclosure, disruption, modification, or destruction** in order to provid

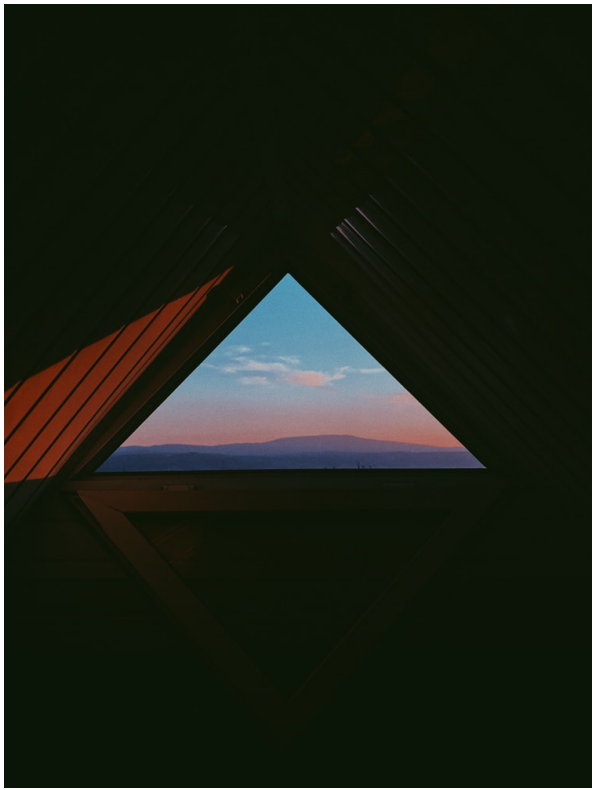
- (A) **integrity**, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- (B) **confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- (C) **availability**, which means ensuring timely and reliable access to and use of information.

https://www.law.cornell.edu/uscode/text/44/3542

The CIA triad

The “CIA triad.” CIA stands for:

- **Confidentiality** through preventing access by unauthorized users.
- **Integrity** from validating that your data is trustworthy and accurate.
- **Availability** by ensuring data is available when needed.



https://www.ibm.com/blogs/cloud-computing/2018/01/16/drive-compliance-cloud/

CIA triad example

The CIA triad

Situation: General hospital and a specialised hospital. A patient has to be transferred to the specialised hospital. Of course all available information about the patient should be transferred from the General hospital to the specialised hospital.

From the CIA point of view:

- **Confidential**: Nobody except the recipient (Doctor) is able to read it
- **Integrity**: The information is fully transferred and no data has been altered
- **Availability**: The systems to which the Doctors / employees will access the data, have to beeen available

Methods used to ensure Confidentiality

- Data encryption and authentication
- Encryption of the data in transit
- Using User IDs, passwords and other methods to access the encrypted data
  - 2 FA / MFA as previously discussed (Hardware tokens, biometric verification, …)
- Extra measures (extreme form): Air gapped computers, disconnected storage devices hard copy only

Methods used to ensure Integrity

- Maintaining the **consistency**, **accuracy**, and **trustworthiness** of data over its entire life cycle
- Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people
  - File permissions and user access controls
  - Version Control Systems
- Detect changes
  - Cryptographic checksums

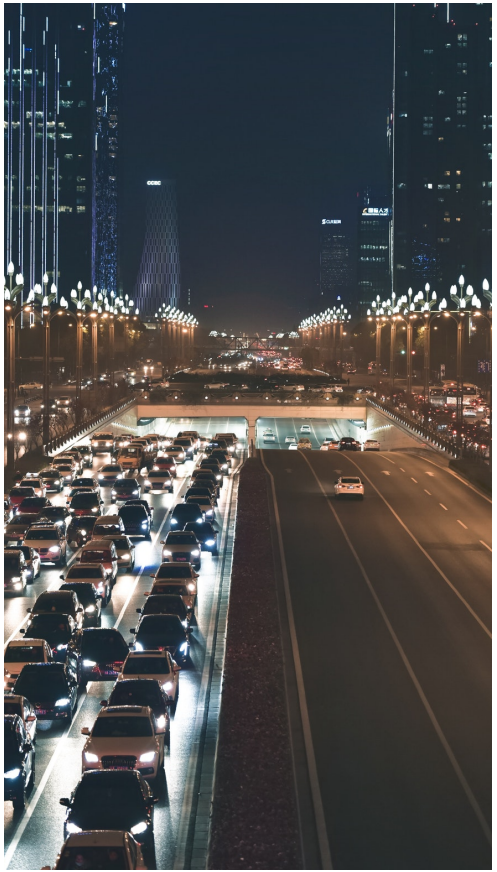
Methods used to ensure Integrity

- **HMAC**: **Hash-based message authentication code**
- Is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key
- ~~MD5~~, SHA-256, SHA-3, …

```
macbook:~ seitz$ echo -n "Hi all" | shasum -a 256
e6cf54f1c0d4ec54e879ae23f41f87c7361550d7b385d20bd2ba4e9c6064a71a  -
macbook :~ seitz$ echo -n "Hi all" | shasum -a 256
005a9b72487248c324348c754b7b7a695dd6b98aa0058ff6363f365763d11e8d  -
```

Methods used to ensure Availability

- Redundant hardware
- Fully maintained hardware
- Keep current with all necessary system upgrades and updates
- Ensure to have enough bandwidth to and from the systems
- Remove bottlenecks
- Hot failover
- RAID
- Planed (Disaster recovery plan - DRP) and trained disaster recovery.
- Backups
  - Geographically-isolated location
  - Fireproof, waterproof safe
- Measures against DDoS



Authentication and Authorisation

- **Authentication (Who you are)**: The process of determining whether someone or something is who or what it declares itself to be.
  - "Are you really student X?"
  - Technical methods: Login Form, HTTP authentication, HTTP digest, X.509 certificate, …
- **Authorisation (What you can do)**: Decides if you have permission to access a resource
  - Methods: Access controls for URLs, Secure objects and methods, Access control lists (ACLs)

Authentication and Authorisation

Factors for Authentication

- Something you **know**
  - Operating system password
  - Credit Card PIN
  - Safe pin
  - Smartphone unlock combination
  - Secret handshakes

Factors for Authentication

- Something you **have**
  - Physical objects
  - Keys
  - Smartphones
  - Smart Cards
  - USB drives
  - Token devices

Factors for Authentication

- Something you **are**
  - Fingerprint
  - Palm
  - Iris
  - Retina
  - Blood
  - DNA

Factors for Authentication

- **(Somewhere** you are)
  - Related to your location
  - IP address

Factors for Authentication

- **(Something** you do)
  - Gestures
  - Related to something you know

Multifactor authentication (MFA)

- Combining two or three factors from the previous categories
- More secure because an attacker needs multiple skills to breach an account
- Attacker needs to perform **multiple successful attacks simultaneously**
- Famous example: 2FA
- If available: You should use 2FA

Multi factor authentication - Examples

Paper: “Evaluating Login Challenges as a Defense Against Account Takeover”

“In this paper, we study the efficacy of **login challenges** at **preventing account takeover** …. These secondary authentication … trigger in response to a suspicious login or account recovery attempt. Using Google as a case study … preventing over 350,000 real-world hijacking attempts stemming from automated bots, phishers, and targeted attackers. We show that knowledge-based challenges prevent as few as 10% of hijacking attempts rooted in phishing and 73% of automated hijacking attempts. **Device-based challenges provide the best protection, blocking over 94% of hijacking attempts rooted in phishing and 100% of automated hijacking attempts**.”

https://ai.google/research/pubs/pub48119

Google’s automatic, proactive hijacking protection

“if we **detect** a **suspicious sign-in attempt** (say, from a new location or device), we’ll ask for **additional proof** that it’s really you. This proof might be confirming you have access to a trusted phone or answering a question where only you know the correct response.“

“If you’ve signed into your phone or set up a recovery phone number, we can provide a similar level of protection to 2-Step Verification via device-based challenges. We found that an **SMS code sent to a recovery phone number helped block 100% of automated bots, 96% of bulk phishing attacks, and 76% of targeted attacks**. **On-device prompts, a more secure replacement for SMS, helped prevent 100% of automated bots, 99% of bulk phishing attacks and 90% of targeted attacks.**“

https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Google’s automatic, proactive hijacking protection

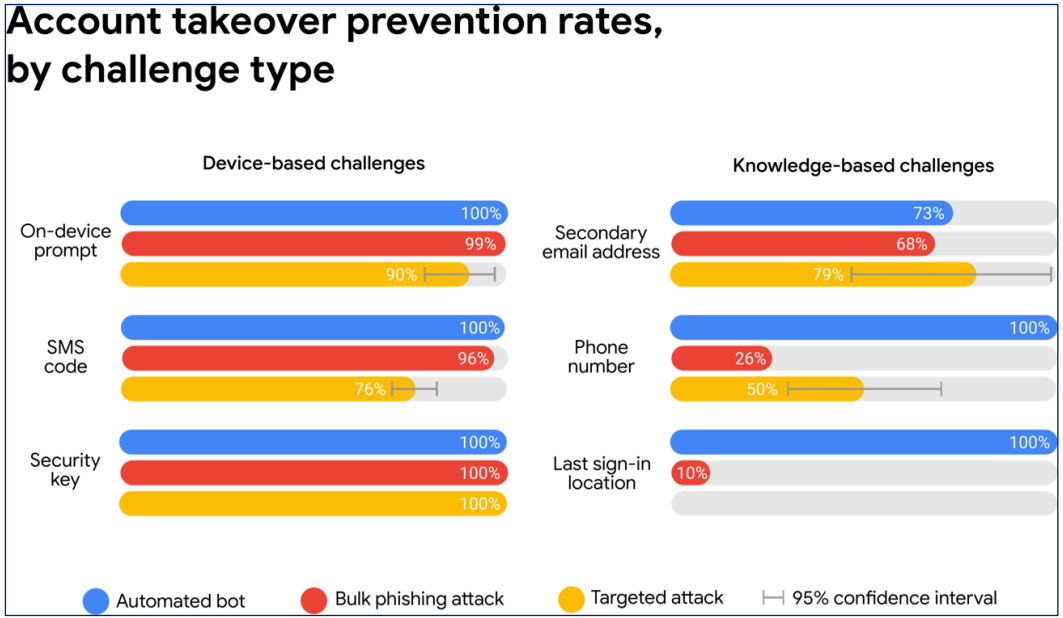


Image Source: https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Password Cracking

- Passwords should be stored as Hashes
- Here Example of Linux Password:

test:6n/L4kZYI$tKLzmKZSU85laE6lIUjpUP[…]:18058:0:99999:7:::

SHA512 SALT Hashed Password LastSet MinMax PW Age Day PW Remind

- Salt adds complexity to Crack

Method of Password Cracking

- Brute Force
- Dictionary Attack
- Rainbow Tables (before SALT was added)
- Rule Based Dictionary | Brute Force

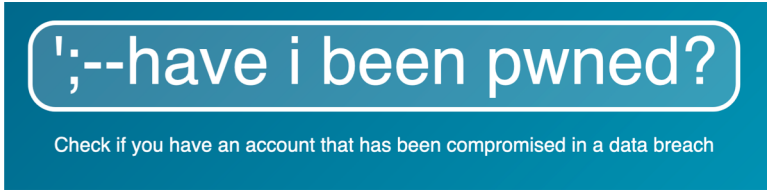
Top 10 Passwords used 2019

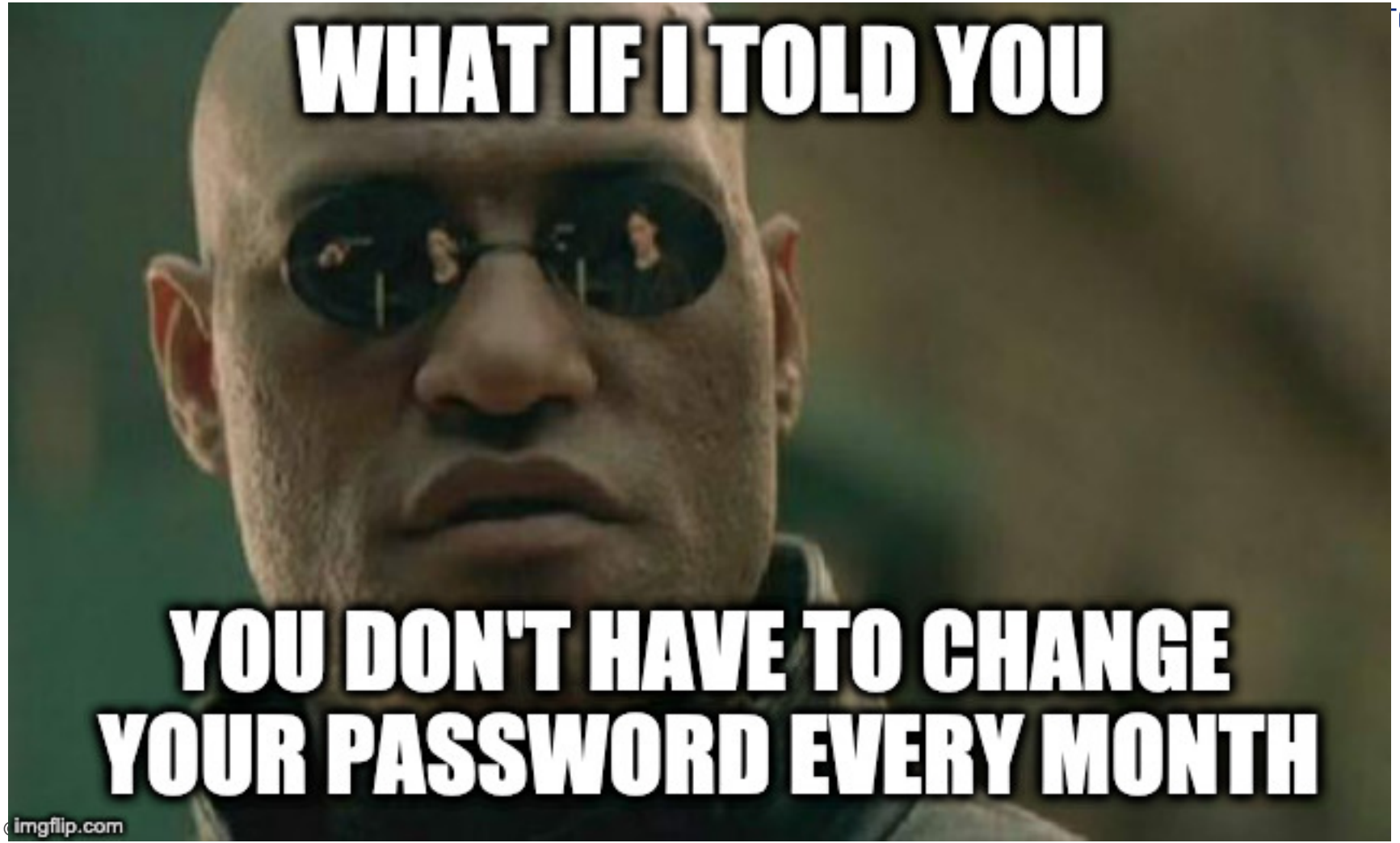
1. 123456
2. 1234
3. 123456789
4. 1234578
5. 12345
6. 111111
7. hallo
8. passwort
9. soleil
10. password

Demo: Password check and hack

- HashCat

- Have I been pawned?




WHAT IF I TOLD YOU
YOU DON'T HAVE TO CHANGE YOUR PASSWORD EVERY MONTH
imgflip.com

New NIST Standards

- Use longer passwords
- No Passwords Expire (without Reason)
- No Composition Rules (Signs, Numbers, Big Letters)
- Do Check your password against compromised lists
- Use a Password Manager

Additional Consideration

- Use Role Based Access Controls
- Log every authentication attempt (failed and successful)
- Use Second Factor

2 Factor Authentication

- Having two passwords doesn’t count
  - Something you have (token)
  - Something you know (password)
  - Something you are (biometric)

- Yubikey
- Google Authenticator
- SMS (deprecated!)

Entropy (information theory)

- Information entropy is measured in bits
- Strength of a password is measured with Entropy bits (Log2)
- Example:
  - Password policy: Length of the password must be 8 characters and has to contain a special character and is case-sensitive
  - Possibilities per character: 29 (uncapitalised) + 29 (capitalised) + 11 special characters (!” $%&/()=?)
    = 69 possibilities per character

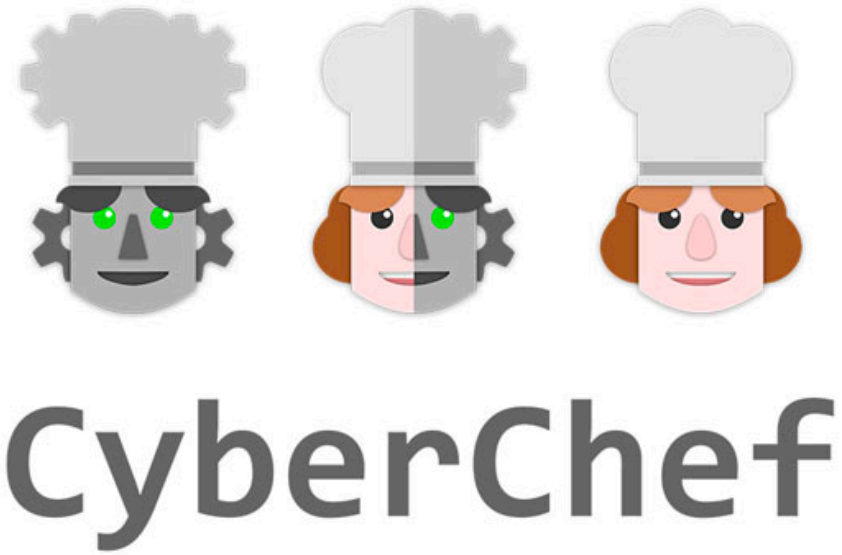
Log2(69) = 6,1 Bit entropy per character

Password strength = 8 * 6.1 = 48.9 bits

Entropy (information theory)

- Calculate the password strength of the following two passwords
  - 10 characters, a-z and A-Z are allowed
  - 7 characters, a-z, A-Z and 0-9 are allowed

Demo: Entropy with CyberChef



Cryptology Where used in daily life?

Task:

Take a Website and look at the Certificate.

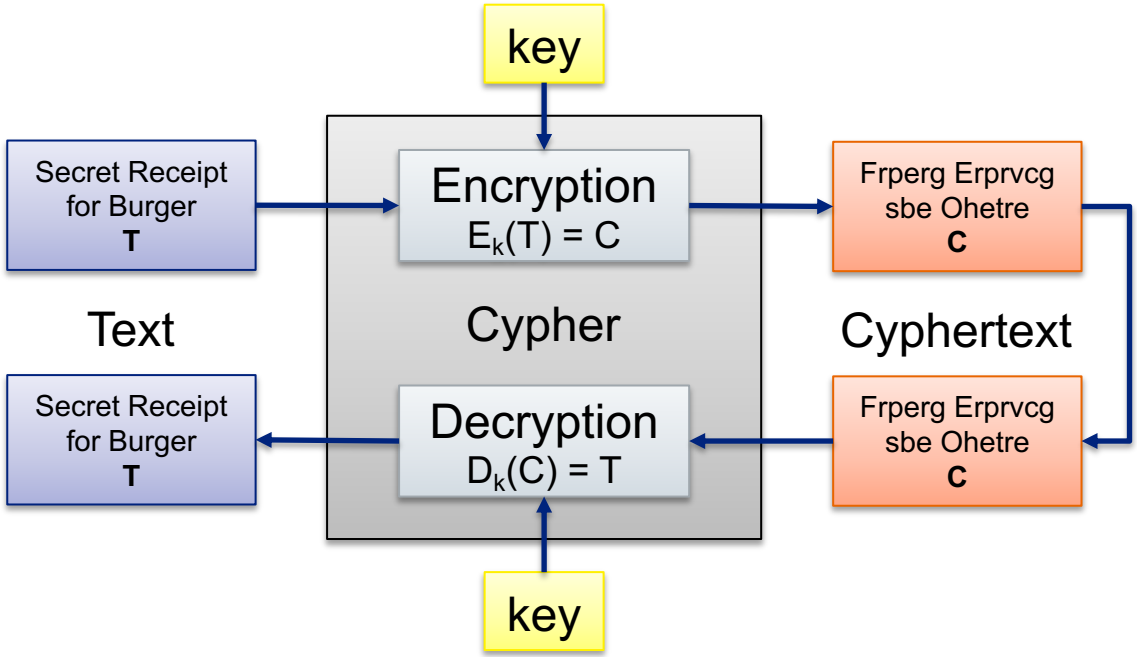
What Ciphers are they using? Try to find out…

Cryptology Definition

Cryptology	
Cryptography	Cryptoanalysis
The art and science of **creating** ciphers	The art and science of **braking** ciphers

What is a Cipher?

- Algorithm to encrypt (or decrypt) a Message



Cryptographic Algorithms

Algorithms		
Symmetric	Asymetric	Hash
One Cipher and Key to Encrypt and Decrypt Data	Cipher with a Public and Private Key to Encrypt and Decrypt Data	Checksum of Data to prove consistency

Basic Encryption

- Text
  “We are here at UniBe learning about Security”

- Encrypted
  “Jr ner urer ng HavOr yrneavat nobhg Frphevgl”

Question / Task:

Any Idea what Cipher is used?

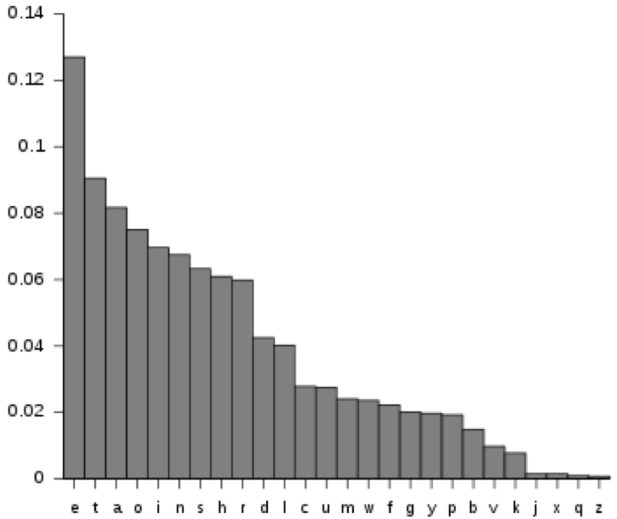
ROT13 and Cryptoanalysis

- Overlaying the Text, easy to find similarities
  “We are here at UniBe learning about Security”
  “Jr ner urer ng HavOr yrneavat nobhg Frphevgl”

- ROT13 Cipher (rotate by 13)
- Encryption and Decryption with same algorithm (and option)

Distribution in the Text

- e: 7
- ␣: 7
- a: 4
- r: 4
- t: 3



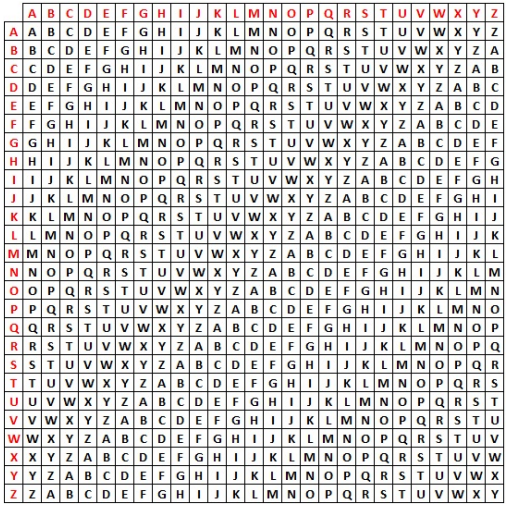
Task:

Do you have an idea to make it more complex?

Vigenere

```
Weareh|ereatU|niBele|arning|aboutS|ecurit|y
SWITCH|SWITCH|SWITCH|SWITCH|SWITCH|SWITCH|S
```

```
Oaikgo wnmtvB feJxnl snvbpn sxwnvZ wyckka q
```



Task:

Do you have an idea to make it more complex?

XOR on Binary Level (switch bit if Key is 1)

```
T: 01010011010101111010010010101010001000011010010000
K: 01010100010110010101001001001001010011111010011110

C: 00000111100001111000011011000111010000110000000110
```

Question:

What is special at this example?

Some VIPs in Cryptology

- (9 c.) Al Kandi (Decipher Messages with Frequency Analysis)
- (14 c.) Battista Alberti (Polyalphabetic Ciphers)
- (19 c.) Edgar Allan Poe (Known for Cryptoanalysis, wrote a book)
- (WW II) Alan Turing (Decipher Enigma)
- (1948) Claude Shannon (Entropy, Secure Communication)
- (1976) Withfield Diffie and Martin Hellmann (Asymetric Keys)

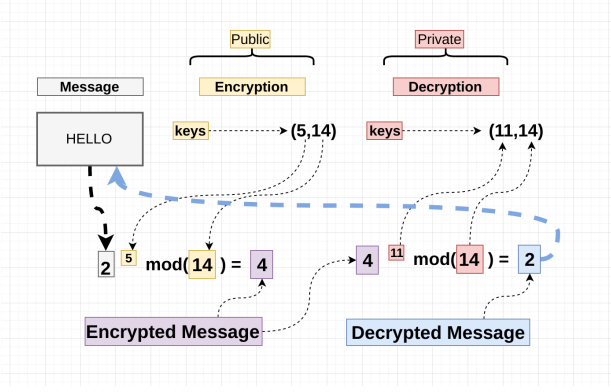
What is used today?

- ECDSA / RSA (Asymmetric Cipher)
- AES-128 (Symmetric Cipher)
- SHA-2 (Hashing Algorithms)

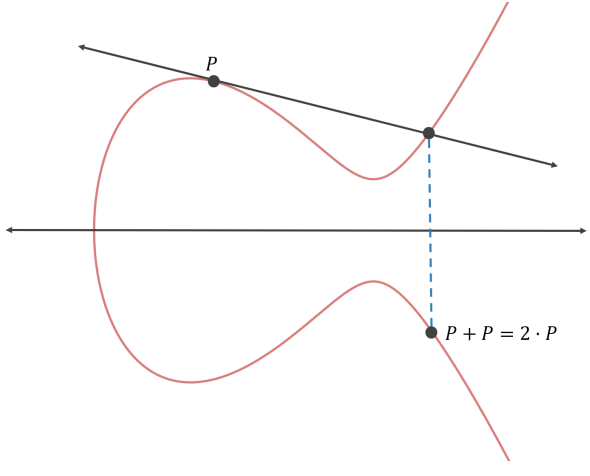
- SHA512 (Linux Passwords)

Asymmetric Ciphers (RSA)

- RSA (Rivest/Shamir/Adelaid)
  - Secured by Factorization Problem
  - Exchange Exponent (Secret two Primes)
  - Big Key Size



- ECDSA
  - Secured by extreme amount of Points (2^256)
  - Exchange Curve Point X=x*P (Secret **x**)
  - Relative small Key Size



Source of current Information

- NIST (National Institute of Standards and Technology US)
- BSI (Bundesamt für Sicherheit in der Informationstechnik)

Excercise: Encrypt and Hack

- Group up in Teams of two Members
- Write a Text and Use a Cesar Cipher
- Give it to your Neighbor group
- Try to Hack the Text

Future of Cryptology

- Quantum Computer will bypass Prime Factorization Problem
- D-Wave currently can factorizing a 17 bit Number
  (Far away from 2048 Bit)

- New Quantum Cryptography brings new possibilities

IT Security Threats

Ransomware

Spam

Web Application Attacks

Malware

Information Leakage

Botnets

Physical manipulation

Phishing

Denial of Service

Cyber Espionage

Cryptojacking

Data Breaches

Identity Theft

Insider Thread

Question:

What do you think are the biggest three Threats?

ENISA Report

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	⇧	2. Web Based Attacks	⇧	→
3. Web Application Attacks	⇧	3. Web Application Attacks	➲	→
4. Phishing	⇧	4. Phishing	⇧	→
5. Spam	⇧	5. Denial of Service	⇧	↑
6. Denial of Service	⇧	6. Spam	➲	↓
7. Ransomware	⇧	7. Botnets	⇧	↑
8. Botnets	⇧	8. Data Breaches	⇧	↑
9. Insider threat	➲	9. Insider Threat	⇩	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	⇧	11. Information Leakage	⇧	↑
12. Identity Theft	⇧	12. Identity Theft	⇧	→
13. Information Leakage	⇧	13. Cryptojacking	⇧	NEW
14. Exploit Kits	⇩	14. Ransomware	⇩	↓
15. Cyber Espionage	⇧	15. Cyber Espionage	⇩	→

Legend: Trends: ⇩ Declining, ➲ Stable, ⇧ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

What we will/have talked about today…

Ransomware

Spam

Web Application Attacks

Malware

Information Leakage

Botnets

Physical manipulation

Phishing

Denial of Service

Cyber Espionage

Cryptojacking

Data Breaches

Insider Thread

Identity Theft

Type of Attacks

- One Shot Stealing Information (phishing)
- Money Cows (Fraud)
- Hijacking Machines (Botnet, Malware)
- Cryptolocker (Ransomewaree)
- Advanced Persistent Threads (specific like Stuxnet)

Phishing

Phishing

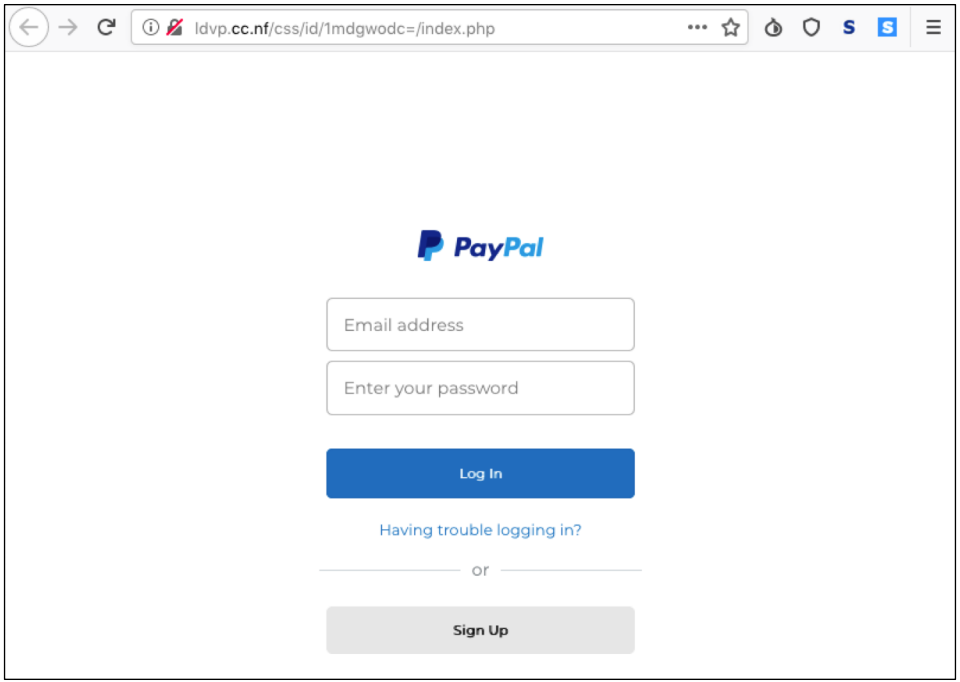
“Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution **to lure individuals into providing sensitive data** such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can **result in identity theft and financial loss**.”

http://www.phishing.org/what-is-phishing

“The word "phishing" comes from the analogy that Internet scammers are using email lures to "fish" for passwords and financial data from the sea of Internet users. The term was coined in the 1996 timeframe by hackers who were stealing America On-Line accounts by scamming passwords from unsuspecting AOL users.”

https://docs.apwg.org/word_phish.html

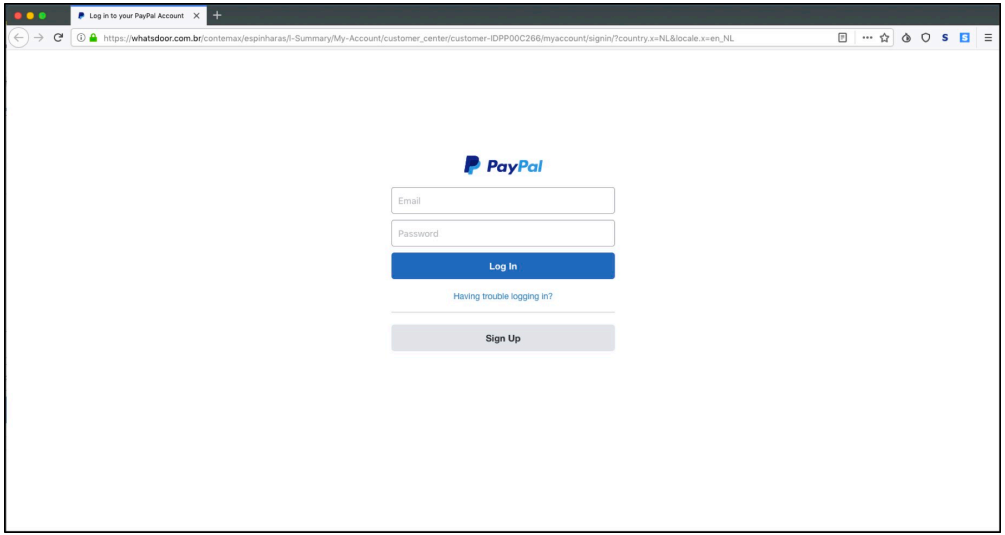
Phishing


ldvp.cc.nf/css/id/1mdgwodc=/index.php
PayPal
Email address
Enter your password
Log In
Having trouble logging in?
or
Sign Up

Phishing Types

- Generic Phishing
- Spear Phishing
- CEO Fraud / Whale Phishing

Generic Phishing Attack



- Mass sending: Send to thousands of other victims
- Language / cultural border
- The goal is typically to gain Credit Card infos or credentials for further attacks

Spear Phishing Attack

- Spear phishing is a targeted attempt to steal credentials from a specific individual
- The individual is typically scouted during target research and identified as a possible asset for infiltration
- Spear phishing attempts use malware, keylogger, or email to get the individual to give away the credentials
- Typically part of a bigger attack. Credential stealing for an APT (More info on next slide)

APT – Advanced Persistent Threat

- Long-term operations designed to infiltrate and/or exfiltrate valuable data without being discovered
- Very few, but targeted victim (group)
- Example Stuxnet
  - In development since at least 2005
  - Stuxnet targets SCADA systems
  - Responsible for causing substantial damage to
  - Worm is believed to be a jointly built American / Israeli cyberweapon

APT – Advanced Persistent Threat

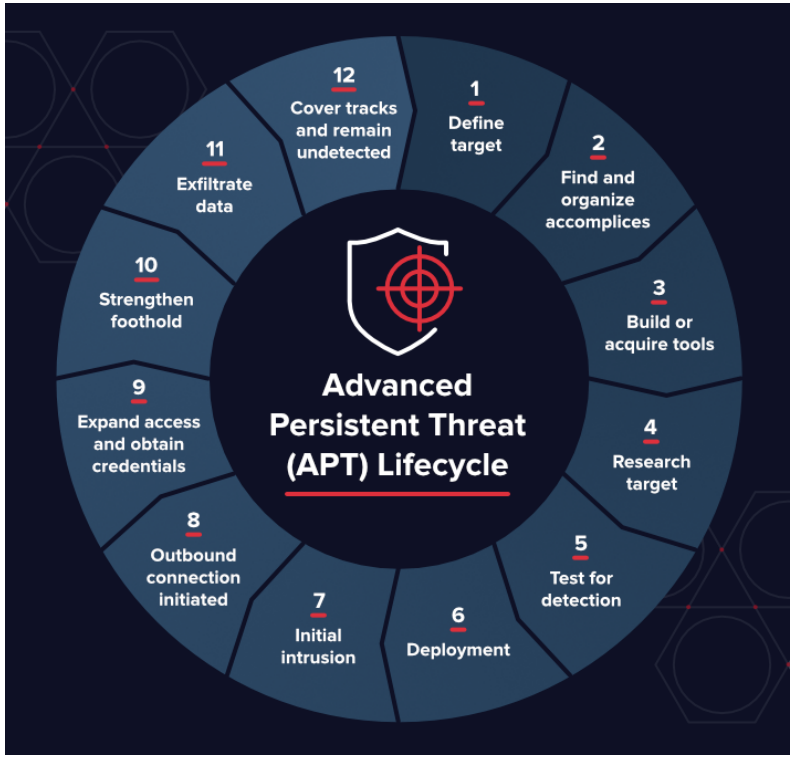


Image Source:
https://www.varonis.com/blog/advanced-persistent-threat/

APT – Advanced Persistent Threat

- Different Names per APT group, depends on the IT security vendor. There is no standard
- As an example, from FireEye:

  APT Groups: APT40 | APT39 | APT38 | APT37 | APT34 | APT33 | APT32 | APT30 | APT29 | APT28 | APT19 | APT18 | APT17 | APT16 | APT12 | APT10 | APT5 | APT3 | APT1

  https://www.fireeye.com/current-threats/apt-groups.html

APT – Advanced Persistent Threat

APT40

- **Suspected attribution**: China
- **Target sectors**: APT40 is a Chinese cyber espionage group that typically targets countries strategically important to the Belt and Road Initiative …
- **Overview**: FireEye Intelligence believes that APT40's operations are a cyber counterpart to China's efforts to modernize its naval capabilities; …
- **Associated malware**: APT40 has been observed using at least 51 different code families. Of these, 37 are non-public. At least seven of these non-public tools (BADSIGN, FIELDGOAL, FINDLOCK, PHOTO, SCANBOX, SOGU, and WIDETONE) are shared with other suspected China-nexus operators.
- **Attack vectors**: APT40 typically poses as a prominent individual who is probably of interest to a target to send **spear-phishing emails** …

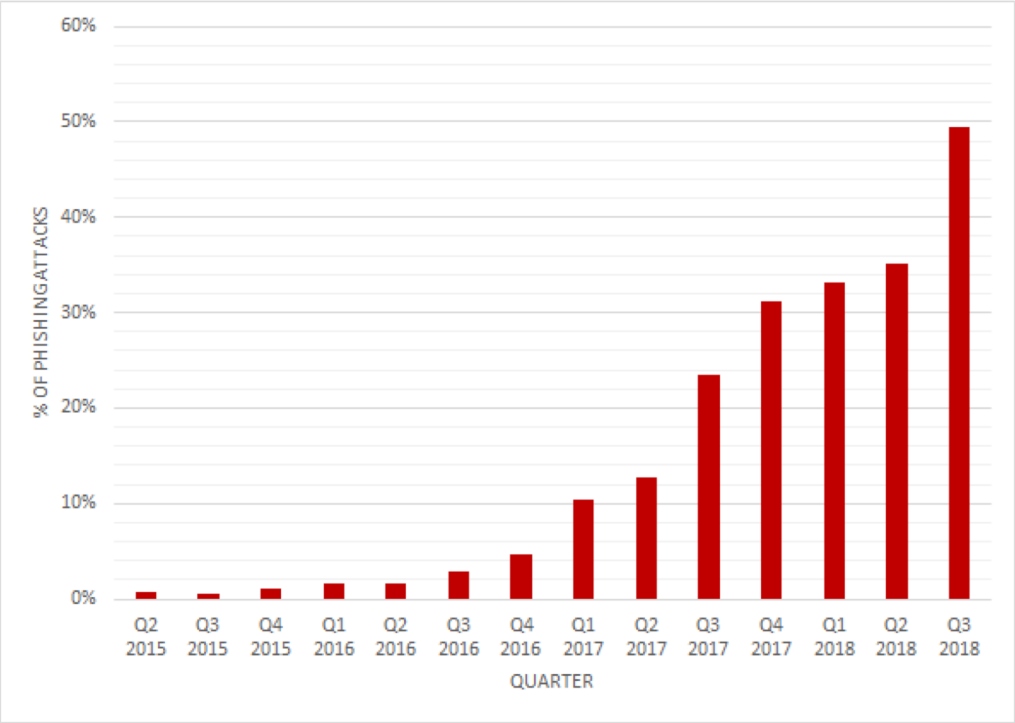
Whale Phishing

- Phishing attack that is specifically aimed at wealthy, powerful, or prominent individuals
- Af such a user becomes the victim of a phishing attack he can be considered a “big phish,” or, alternately, a "whale
- Whale phishing involves the same tactics used in spear phishing campaigns
- Also known as CEO Fraud, BEC (Business Email Compromise), FPF (Fake President Fraud) oder Bogus Boss Email

HTTP vs HTTPS

- HTTP stands for Hyper Text Transfer Protocol
- Communication between clients (users) and web servers is done by sending HTTP Requests and receiving HTTP Responses
- HTTP: No Data Encryption Implemented
- Hypertext Transfer Protocol Secure (HTTPS) is an extension of the HTTP protocol. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS)

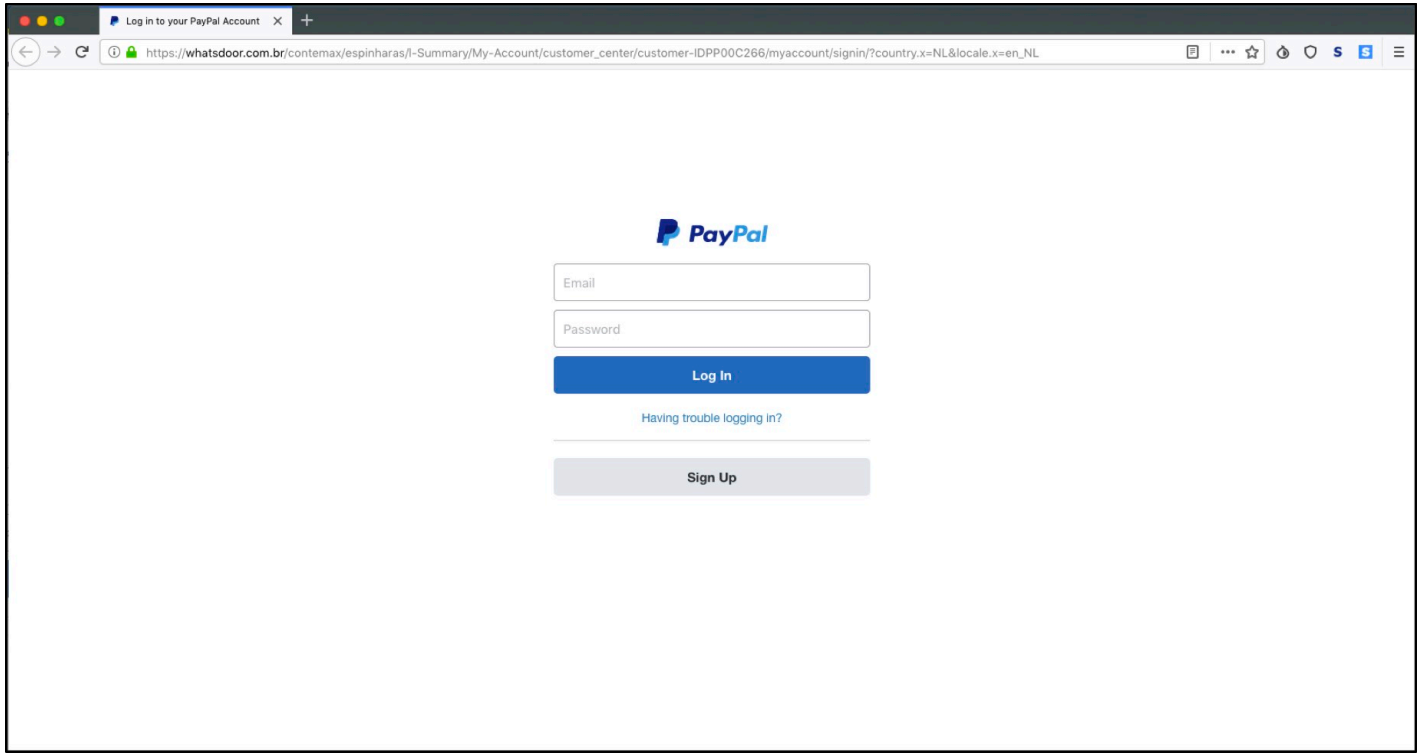
Does HTTPS help against Phishing?



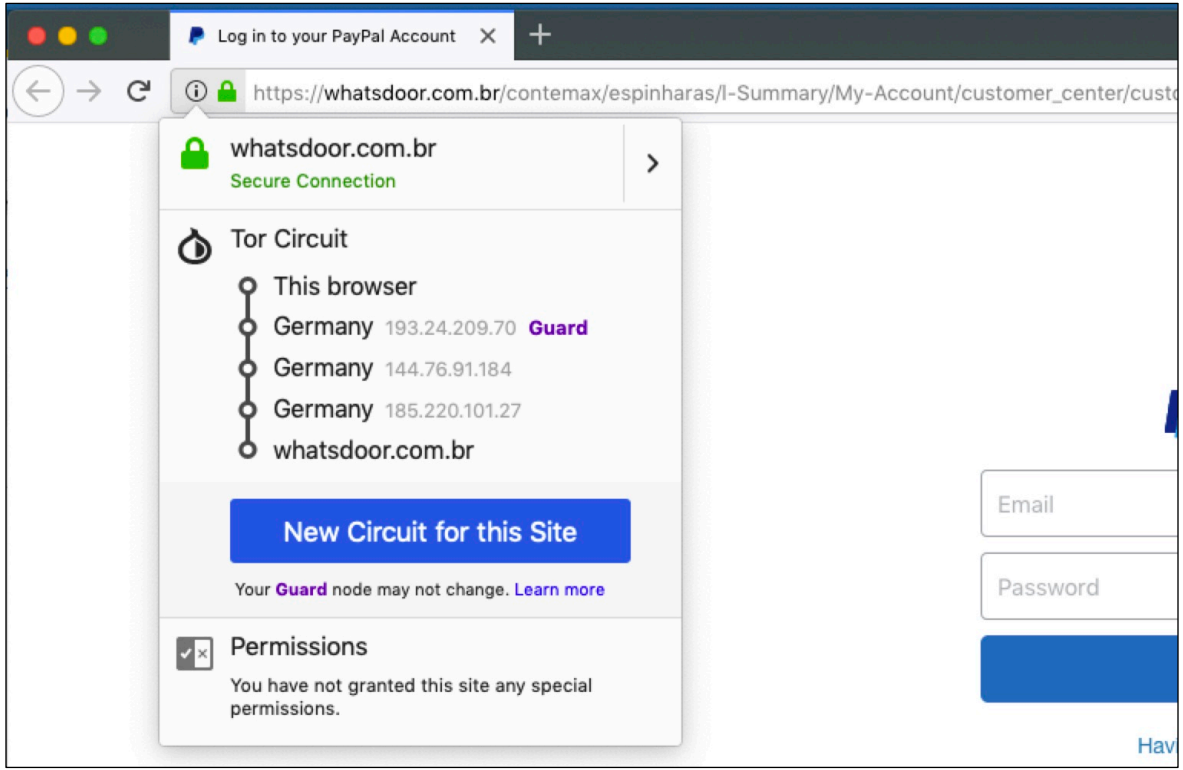
Phishlabs: “49 Percent of Phishing Sites Now Use HTTPS”

Image Source: https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https

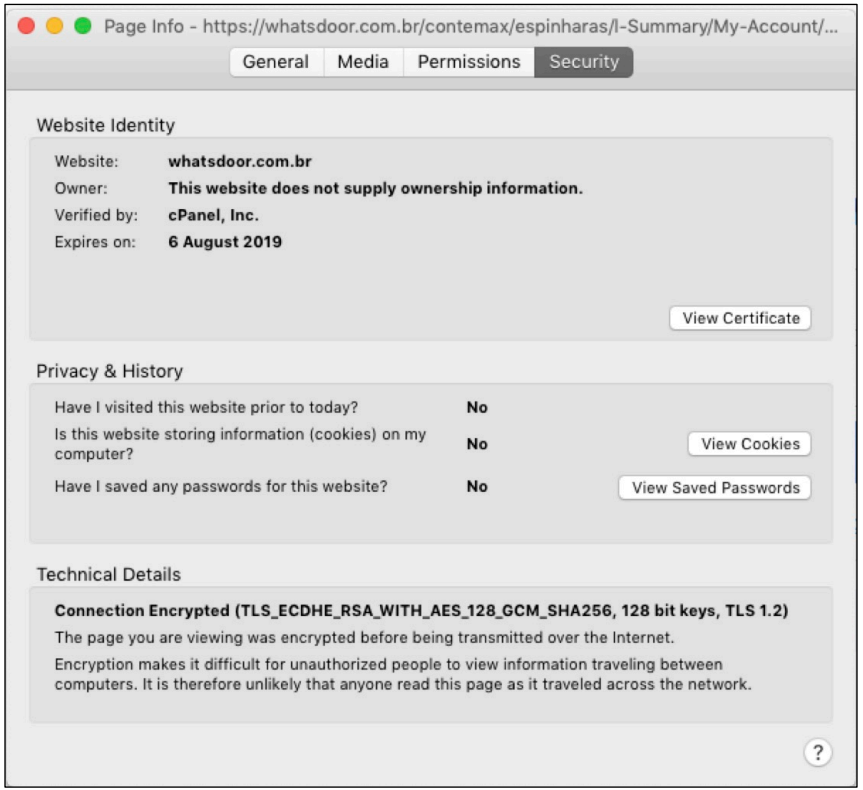
Phishing


Log in to your PayPal Account
https://whatsdoor.com.br/contemax/espinharas/I-Summary/My-Account/customer_center/customer-IDPP00C266/myaccount/signin/?country.x=NL&locale.x=en_NL
PayPal
Email
Password
Log In
Having trouble logging in?
Sign Up

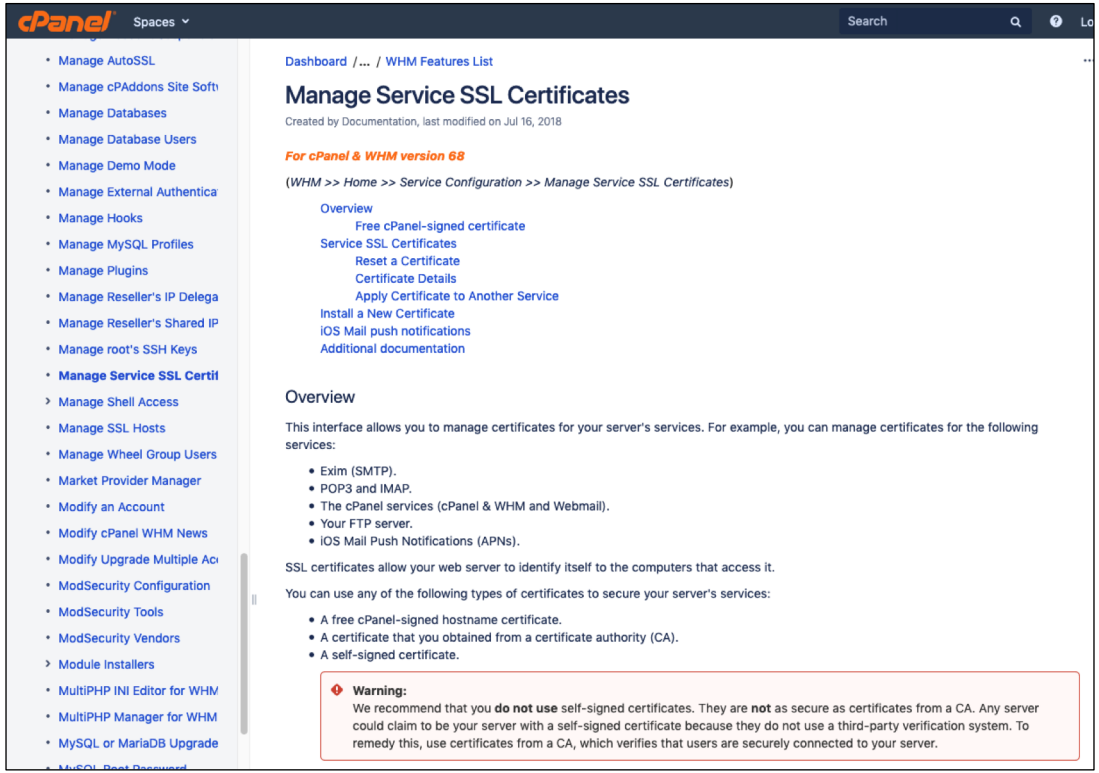
Phishing


Log in to your PayPal Account
https://whatsdoor.com.br/contemax/espinharas/I-Summary/My-Account/customer_center/custo
whatsdoor.com.br
Secure Connection
Tor Circuit
This browser
Germany 193.24.209.70 Guard
Germany 144.76.91.184
Germany 185.220.101.27
whatsdoor.com.br
New Circuit for this Site
Your Guard node may not change. Learn more
Permissions
You have not granted this site any special permissions.
Email
Password
Hav

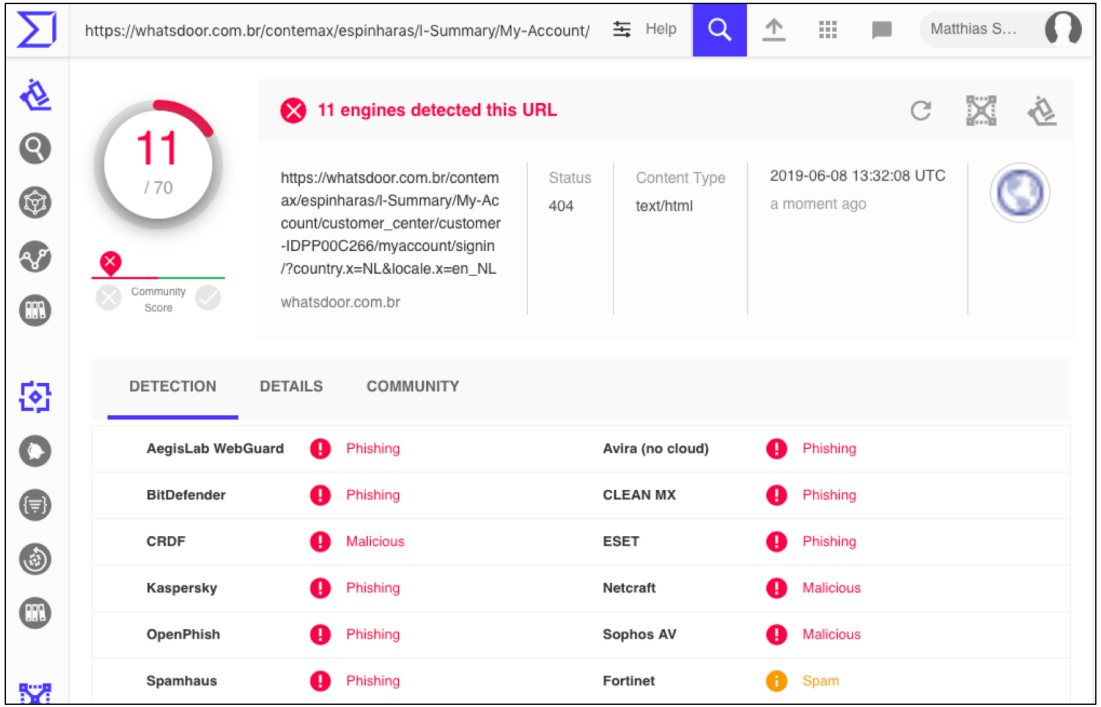
Phishing


Page Info - https://whatsdoor.com.br/contemax/espinharas/l-Summary/My-Account/...
General
Media
Permissions
Security
Website Identity
Website: whatsdoor.com.br
Owner: This website does not supply ownership information.
Verified by: cPanel, Inc.
Expires on: 6 August 2019
View Certificate
Privacy & History
Have I visited this website prior to today? No
Is this website storing information (cookies) on my computer? No
View Cookies
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.
?

Phishing

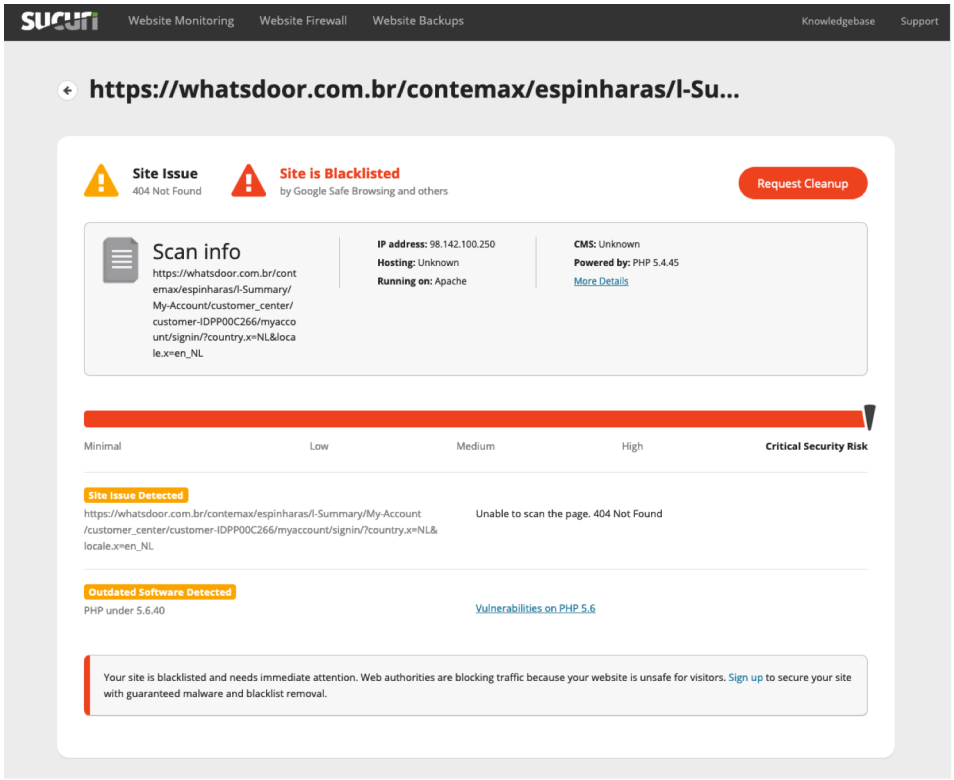

cPanel
Spaces
Search
Manage AutoSSL
Manage cPAddons Site Soft
Manage Databases
Manage Database Users
Manage Demo Mode
Manage External Authentica
Manage Hooks
Manage MySQL Profiles
Manage Plugins
Manage Reseller's IP Delega
Manage Reseller's Shared IP
Manage root's SSH Keys
Manage Service SSL Certif
Manage Shell Access
Manage SSL Hosts
Manage Wheel Group Users
Market Provider Manager
Modify an Account
Modify cPanel WHM News
Modify Upgrade Multiple Ac
ModSecurity Configuration
ModSecurity Tools
ModSecurity Vendors
Module Installers
MultiPHP INI Editor for WHM
MultiPHP Manager for WHM
MySQL or MariaDB Upgrade
Dashboard / ... / WHM Features List
Manage Service SSL Certificates
Created by Documentation, last modified on Jul 16, 2018
For cPanel & WHM version 68
(WHM >> Home >> Service Configuration >> Manage Service SSL Certificates)
Overview
Free cPanel-signed certificate
Service SSL Certificates
Reset a Certificate
Certificate Details
Apply Certificate to Another Service
Install a New Certificate
iOS Mail push notifications
Additional documentation
Overview
This interface allows you to manage certificates for your server's services. For example, you can manage certificates for the following services:
Exim (SMTP).
POP3 and IMAP.
The cPanel services (cPanel & WHM and Webmail).
Your FTP server.
iOS Mail Push Notifications (APNs).
SSL certificates allow your web server to identify itself to the computers that access it.
You can use any of the following types of certificates to secure your server's services:
A free cPanel-signed hostname certificate.
A certificate that you obtained from a certificate authority (CA).
A self-signed certificate.
Warning:
We recommend that you do not use self-signed certificates. They are not as secure as certificates from a CA. Any server could claim to be your server with a self-signed certificate because they do not use a third-party verification system. To remedy this, use certificates from a CA, which verifies that users are securely connected to your server.

Phishing Checks



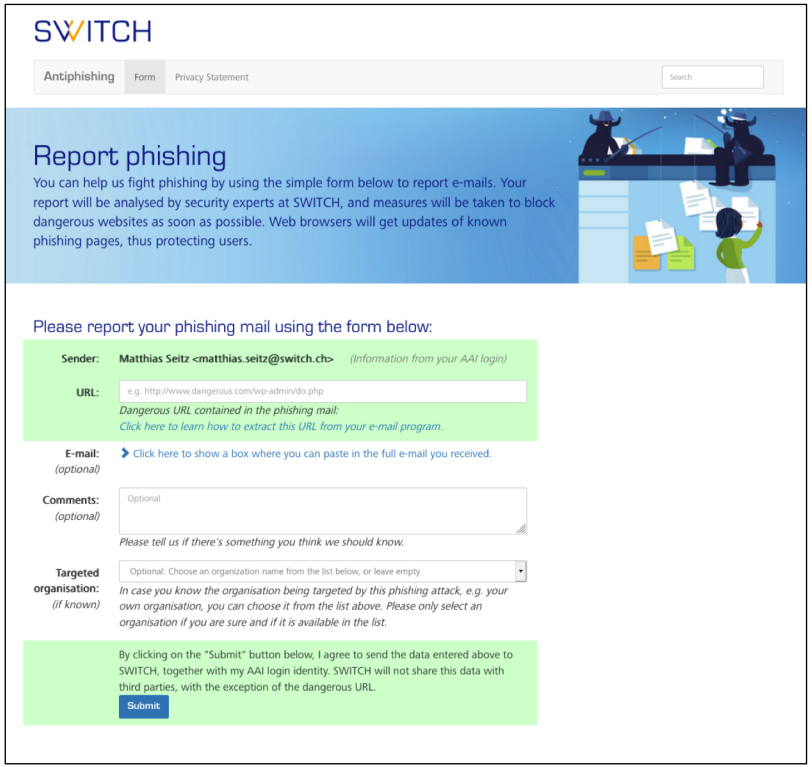
https://www.virustotal.com

Phishing Checks



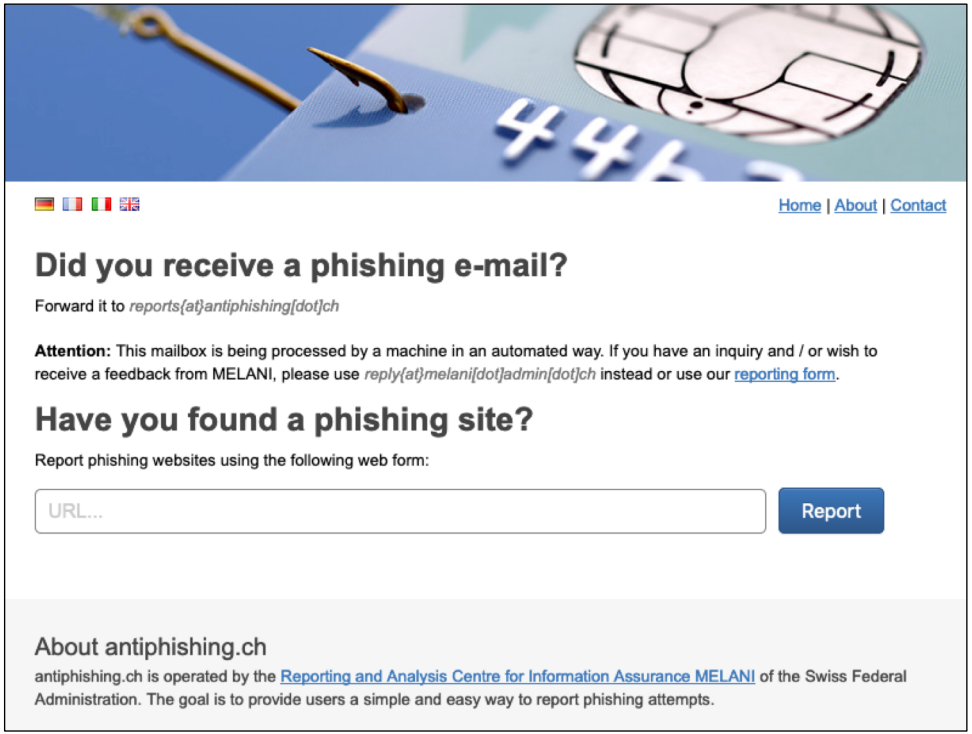
https://sitecheck.sucuri.net/

Report Phishing



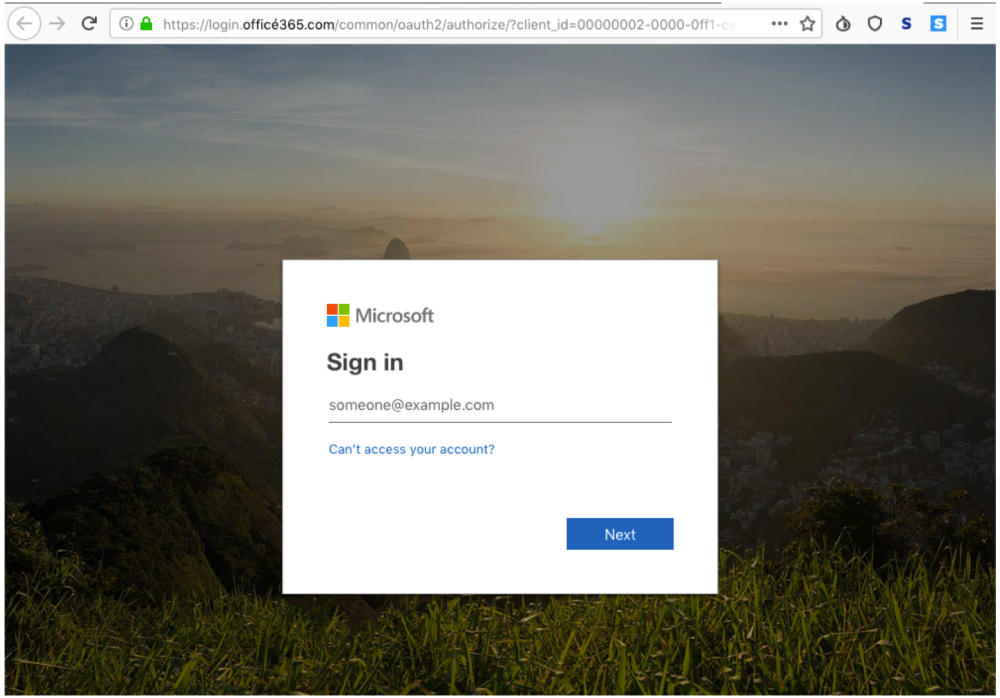
https://www.switch.ch/phishing/report-phishing/

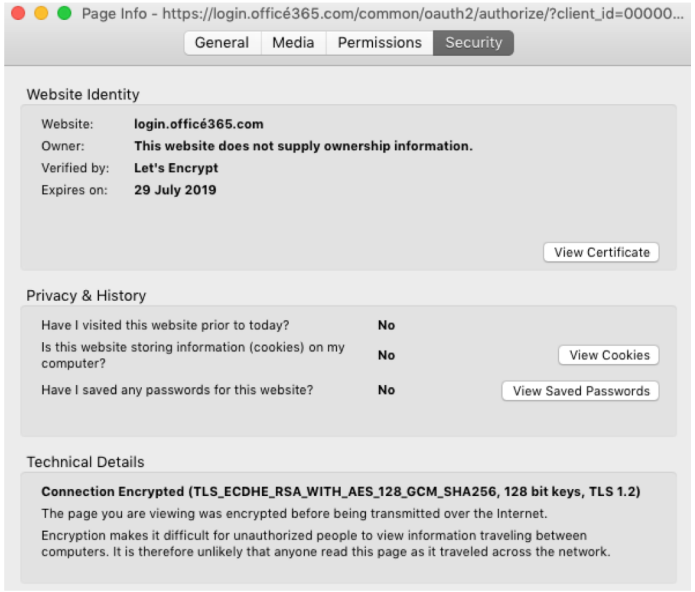
Report Phishing



https://www.antiphishing.ch

Advanced Phishing





Advanced Phishing

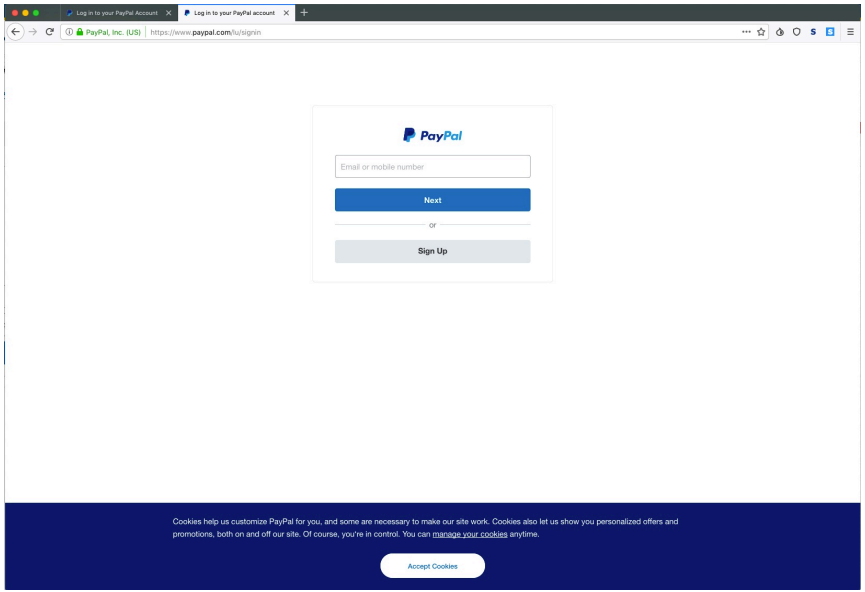
- https://login.xn--offic365-f1a.com

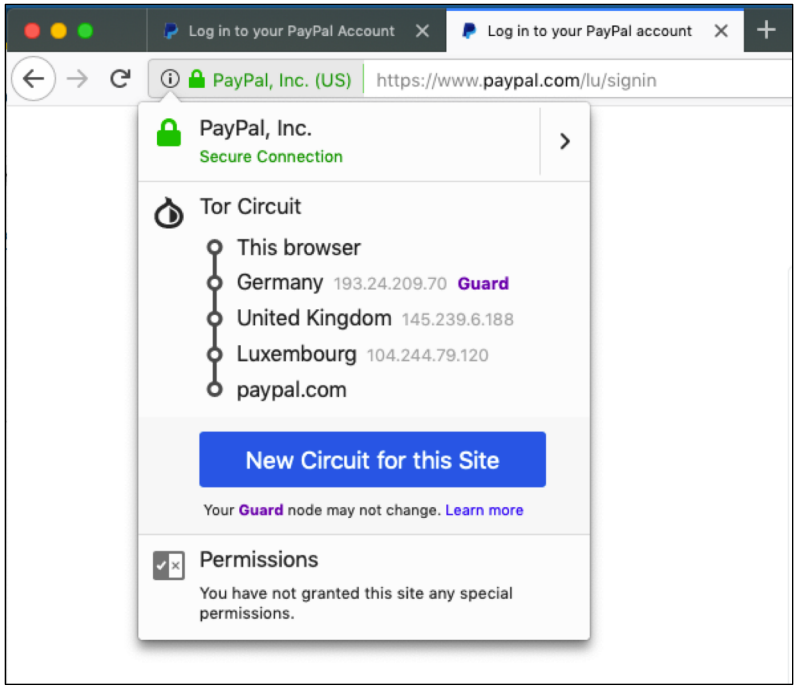
- Punycode
  - Is a way to **represent International Domain Names (IDNs) with the limited character set (A-Z, 0-9)** supported by the domain name system.
  - For example, "münich" would be encoded as "mnich-kva".
  - An IDN takes the punycode encoding, and adds a "xn--" in front of it.
  - "münich.com" would become "xn--mnich-kva.com".
  - Punycode rendering depends on the browser. Firefox will display it as a look-alike domain

Phishing

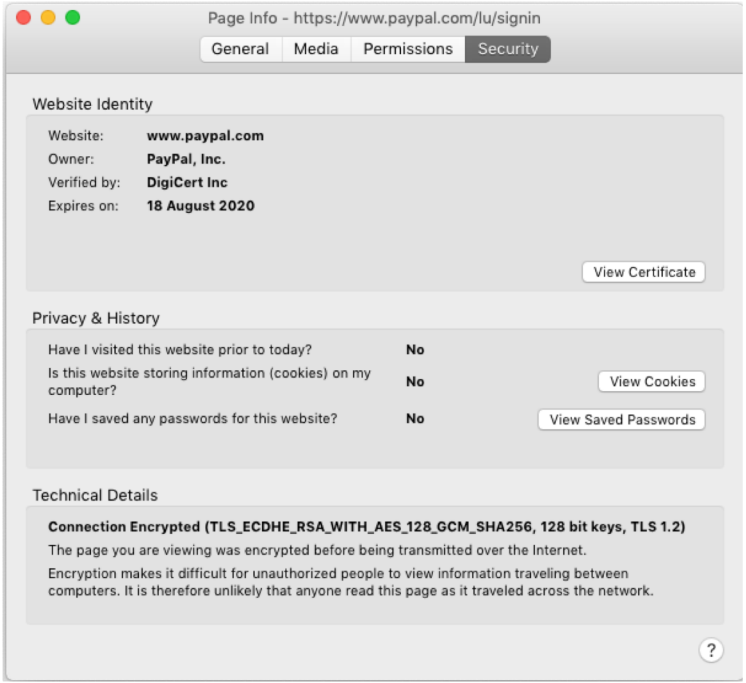
Phishtank Demo

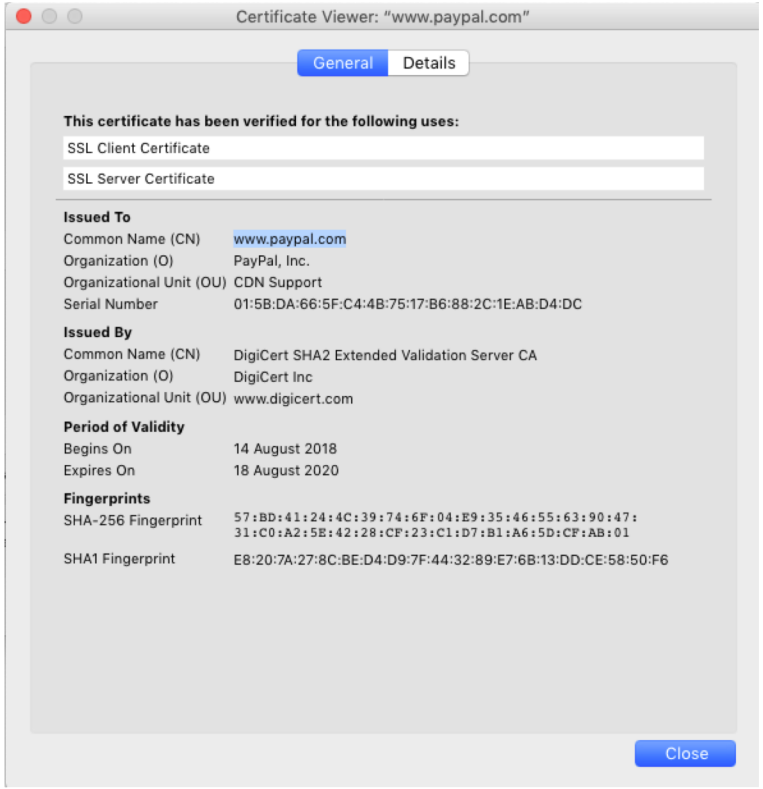
Certificates



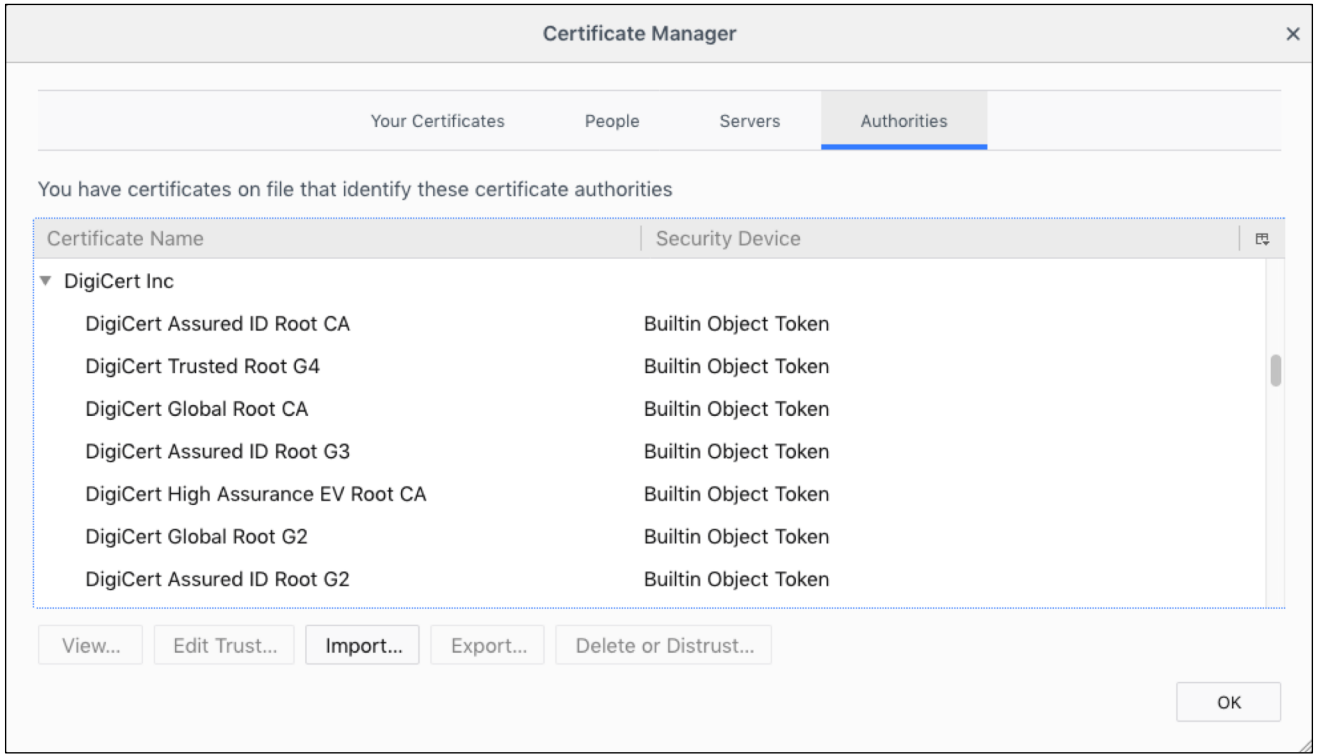


Certificates

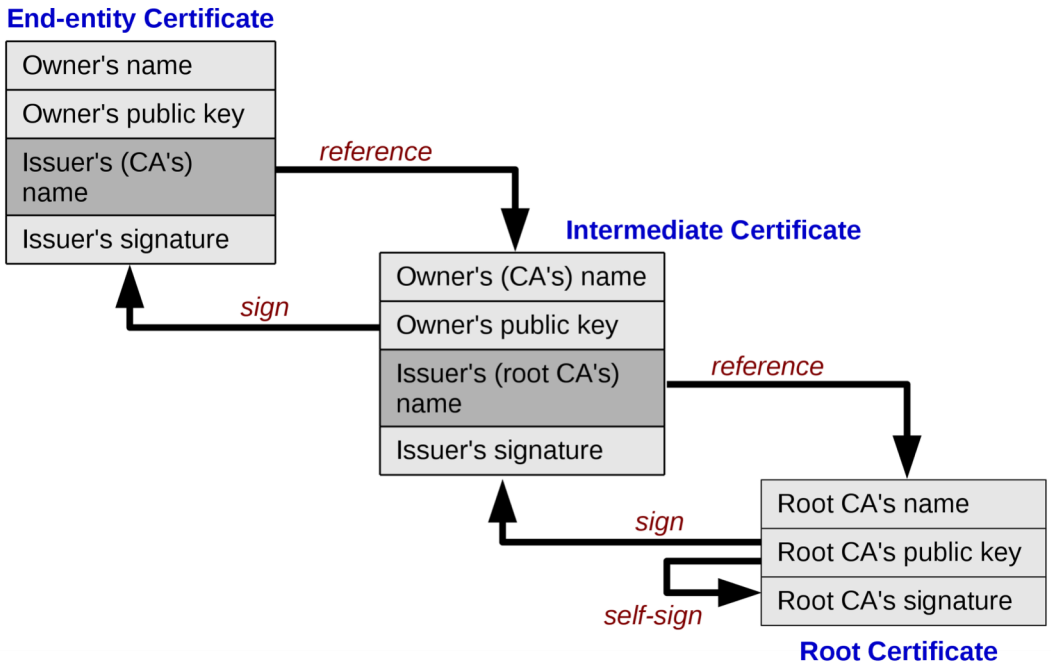




Certificates



Chain of Trust and Root CA's



SSL/TLS Certificate Classes

- Class 1
  - Considered to be **low assurance**
  - Confirms that the Subscriber **controls the asserted email address**
  - **No verification checks** of the Subscriber's **identity** are performed
  - This kind of certificate enables SSL encryption but makes it impossible for users to know the identity
  - This level of validation is referred to as **Domain Validation (DV)**
  - Free

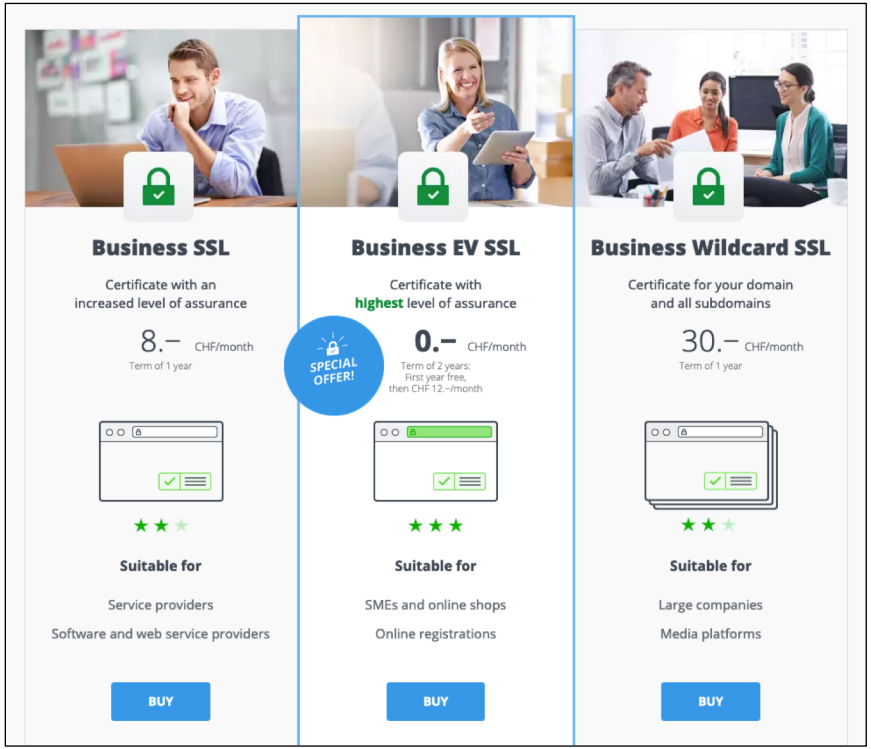
SSL/TLS Certificate Classes

- Class 2
  - Considered to be **medium assurance**
  - Provide a greater level of assurance over Class 1 Certificates
  - **Basic verification steps** to confirm the identity of the Subscriber
  - The certification authority guarantees the existence of the organization, that it owns the associated FQDN
  - One of the organization's manager has authorized the certificate deliverance
  - Referred to as **Organization Validation (OV)**
  - $

SSL/TLS Certificate Classes

- Class 3
  - Certificates provide a **high level of assurance**
  - Issued only after rigorous validation of the identity
  - Those are client certificates that are delivered after an audit that checks the organization and the certificate's owner
  - This level of validation is referred to as **Extended Validation (EV)**
  - $$$

Buy SSL/TLS Certificates



- As an Example – There are plenty of providers
- https://www.hostpoint.ch/en/ssl/ssl-certificate.html

Certificates

Demo 1: Show certificates in browser

Demo 2: SSL Labs

https://www.ssllabs.com/ssltest/

Conficker Experience

- Found infection by Account Locking (Directory Order)
- Analysis of Security-Logs showed infected Machines
- Antivirus Software on Server was stopped
- Fix from Antivirus Vendor were published and used
- Virus was Hopping between Maschines
- It ended up on the Domain Controller it self.

Lessons Learned

- Awareness
- Hardening
- Patch Management
- Operational Security

Examples

- 2008 Conficker in (Multiple: SMB, USB, Network)
- 2010 Stuxnet (USB)
- 2017 EternalBlue (SMB)

Actual Threads

- BlueKeep (RDP)
- Meltdown + Specter (CPU) (since 2018)
- Emotet

- Report on Actual Threads (Martjin van der Heide):

https://www.dropbox.com/s/ds0ra0c8odwsv3m/Threat%20Group%20Cards.pdf?dl

Malware


GovCERT.ch
@GovCERT_CH
Folge ich
Caution: We observed today two Malspam waves distributing eBanking Trojan Retefe. One claimed coming from Lenz & Staehelin and is directed against SMEs, the other targets individuals and pretends to be from a girl in distress. Forward such emails to antiphishing.ch
Tweet übersetzen
:@mbaktconsulting.com>
19
n für
lage gegen Ihre Firma Einsicht
ion ist in der Anlage zur E-Mail
n Sie die Kontaktdaten, die am
hält mich an der Kette im Keller fest....
n den PC auszuschalten und ich habe 3 Min bis er
Webseite geöffnet und habe hier auf Ihre E-Mail
ich bin in Zürich und weiss nicht was weiter gesc
n.
angehängt. Ich flehe um die Hilfe an.
15:49 - 5. Juni 2019

Malware

Von Angela <information@losningsorientert.com>
Antworten
Betreff Hilfe
An
Datum Wed, 5 Jun 2019
Nachrichten-ID losningsorientert.com>
Return-Path <information@losningsorientert.com>
X-Original-To

Ich heisse Angela, 17j, man hält mich an der Kette im Keller fest....
Mein Peiniger hat vergessen den PC auszuschalten und ich habe 3 Min bis er zurückkommt...
ich habe die erste zufällige Webseite geöffnet und habe hier auf Ihre E-Mail gestossen.
Bitte dringend um die Hilfe ich bin in Zürich und weiss nicht was weiter geschieht... Man haut mich jeden Tag.
Informieren Sie meine Eltern.
Ich habe die Infos über sie angehängt. Ich flehe um die Hilfe an.

Von: Lenz & Staehelin <support@mbaktconsulting.com>
Gesendet: Mittwoch, 5. Juni 2019
An: Info
Betreff: Vertraulich: Information für

Sehr geehrte Damen und Herren,
Sie müssen in die gerichtliche Klage gegen Ihre Firma Einsicht nehmen.
Das Dokument mit der Information ist in der Anlage zur E-Mail zu finden.
Für umgehenden Kontakt nutzen Sie die Kontaktdaten, die am Ende des Doku

© 2019 Lenz & Staehelin

Malware

Demo https://hybrid-analysis.com

https://helgrind.switch.ch/joesandbox/index.php/analysis/463786

Emotet Infection @Heise

- June 2019
- Initial infection vector: Email with Emotet malware
- After execution, the malware spread in the whole network
- More sophisticated malware / modules were then loaded
  - Domain controller from Active directory also infected?
  - Trickbot
- Heise decided to full lockdown their network
- External consultants were hired: Incident response and forensic experts
- At least 50’000 Euro damage

- https://www.heise.de/ct/artikel/Trojaner-Befall-Emotet-bei-Heise-4437807.html
- https://www.heise.de/security/meldung/Emotet-bei-Heise-Schaeden-von-weit-ueber-50-000-Euro-4444155.html

Web Application Security

https://www.owasp.org

About OWASP

- The Open Web Application Security Project (OWASP) is an **open community** dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted.

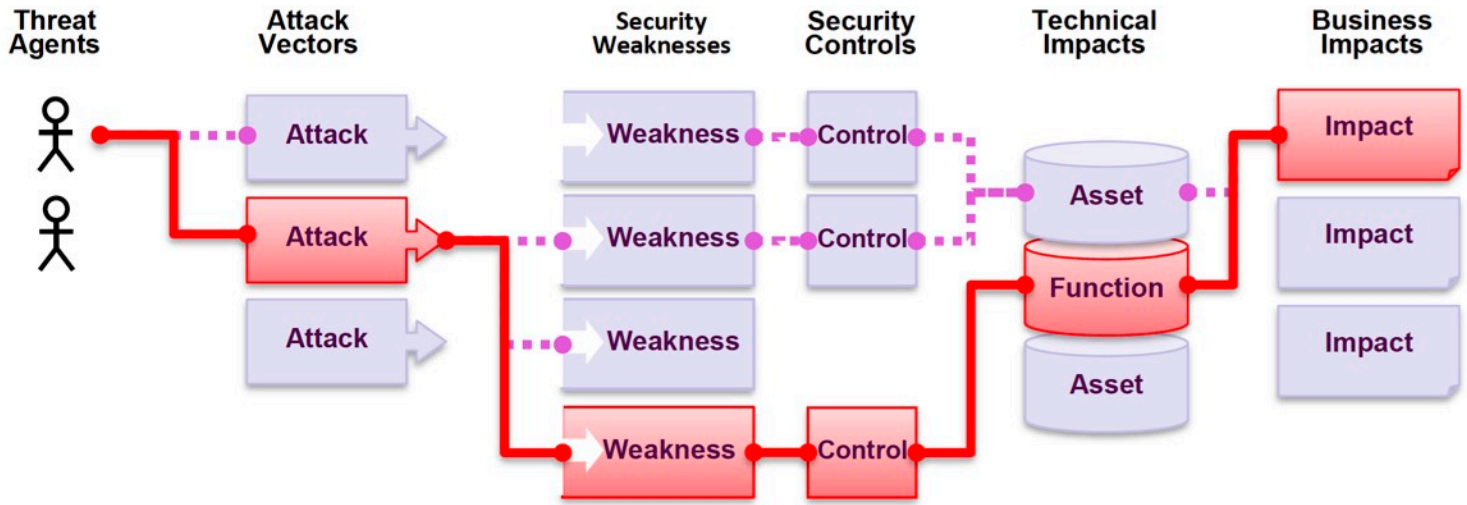
- At OWASP, you'll find free and open:
  - Application security tools and standards.
  - Complete books on application security testing, secure code development, and secure code review.
  - Presentations and videos
  - Cheat sheets on many common topics.

  Learn more at: https://www.owasp.org

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

What Are Application Security Risks?

- **Attackers** can potentially use **many different paths** through your **application** to do harm to your business or organization. Each of these paths represents a **risk** that may, or may not, be serious enough to warrant attention.



What's My Risk?

- The OWASP Top 10 focuses on identifying the **most serious web application security risks** for a broad array of organizations. For each of these risks, we provide generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the OWASP Risk Rating Methodology

Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
Appli-cation Specific	Easy: 3	Widespread: 3	Easy: 3	Severe: 3	Business Specific
	Average: 2	Common: 2	Average: 2	Moderate: 2	
	Difficult: 1	Uncommon: 1	Difficult: 1	Minor: 1	

Web Application Security

Top 3

- A1:2017 Injection
- A2:2017 Broken Authentication
- A3:2017 Sensitive Data Exposure

A1:2017 Injection

- **Problem**: User-supplied data is not validated, filtered, or sanitized by the application (Interpreter)

- Injection flaws are very prevalent, particularly in legacy code. Injection vulnerabilities are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM queries.

- **Impact**: Injection can result in **data loss, corruption, or disclosure to unauthorized parties**, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover. The business impact **depends** on the **needs of the application and data**.

A1:2017 Injection - Example Attack Scenarios

Scenario #1: An application uses untrusted data in the construction of the following **vulnerable** SQL call:

```
String query = "SELECT * FROM accounts WHERE
custID='" + request.getParameter("id") + "'";
```

Scenario #2: Similarly, an application's blind trust in frameworks may result in queries that are still vulnerable, (e.g. Hibernate Query Language (HQL)):

```
Query HQLQuery = session.createQuery("FROM accounts
WHERE custID='" + request.getParameter("id") + "'");
```

In both cases, the attacker modifies the 'id' parameter value in their browser to send: **' or '1'='1**. For example:

```
http://example.com/app/accountView?id=' or '1'='1
```

This changes the meaning of both queries to return all the records from the accounts table. More dangerous attacks could modify or delete data, or even invoke stored procedures.

A1:2017 Injection - Prevention

- The preferred option is to use a **safe API**, which avoids the use of the interpreter entirely or provides a **parameterized interface**
- **Use positive or "whitelist" server side input validation.** This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications.
- Use **LIMIT and other SQL controls** within queries to prevent mass disclosure of records in case of SQL injection.
- For any residual dynamic queries, **escape special characters** using the specific escape syntax for that interpreter.
- For old software / applications: Use a **Web Application Firewall** to filter out the malicious queries

A2:2017 Broken Authentication

- **Problem**: Attackers have access to hundreds of millions of valid username and password combinations for credential stuffing, default administrative account lists, automated brute force, and dictionary attack tools.

- Attackers can detect broken authentication using manual means and exploit them using automated tools with password lists and dictionary attacks

- **Impact**: Attackers have to gain access to only a few accounts, or just one admin account to compromise the system. Depending on the domain of the application, this may **allow money laundering, social security fraud, and identity theft, or disclose legally protected highly sensitive information.**

A2:2017 Broken Authentication – Example Attack Scenarios

- **Scenario #1:** Credential stuffing , the use of **lists** of **known passwords** , is a common attack. If an application does not implement **automated threat** or **credential stuffing protections**, the application can be used as a **password oracle** to determine if the credentials are valid.
- **Scenario #2:** Most authentication attacks occur due to the continued use of **passwords as a sole factor**. Once considered best practices, password rotation and complexity requirements are viewed as encouraging users to use, and reuse, weak passwords. Organizations are recommended to stop these practices per NIST 800 63 and **use multi factor authentication**.
- **Scenario #3:** Application **session timeouts aren't set properly**. A user uses a public computer to access an application. Instead of selecting "**logout**" the user simply closes the browser tab and walks away. An attacker uses the same browser an hour later, and the user is still authenticated.

A2:2017 Broken Authentication – Prevention

- Implement **multi factor authentication** to prevent attacks.
- Do not ship or deploy with **any default credentials**, particularly for admin users.
- Implement **weak password checks**, e.g. against a list of the top 10000 worst passwords
- Align password length, complexity and **rotation policies** with NIST 800 63 B's
- Ensure **registration, credential recovery**, and API pathways are **hardened** against account enumeration attacks by using the same messages for all outcomes.
- **Limit** or increasingly delay **failed login attempts**.
- Use a server side, secure, **built in session manager** that generates a new random session ID with high entropy after login.
- **Session IDs should not be in the URL**, be securely stored and invalidated after logout, idle, and absolute timeouts

A3:2017 Sensitive Data Exposure

- **Problem**: Rather than directly attacking crypto, **attackers steal keys, execute man in the middle attacks, or steal clear text data off the server**, while in **transit**, or from the user's client, e.g. browser. A manual attack is generally required. Previously **retrieved password databases** could **be brute forced** by Graphics Processing Units (GPUs).
- The most common flaw is simply **not encrypting sensitive data**. When crypto is employed, **weak key generation and management**, and weak algorithm, protocol and cipher usage is common, particularly for weak password hashing storage techniques.
- **Impact**: Failure frequently **compromises all data that should have been protected**. Typically, this information includes **sensitive personal information** (PII) data such as health records, credentials , personal data, and credit cards, which often require protection as defined by **laws** or regulations such as the **EU GDPR** or local **privacy laws**.

A3:2017 Sensitive Data Exposure – Example Attack Scenarios

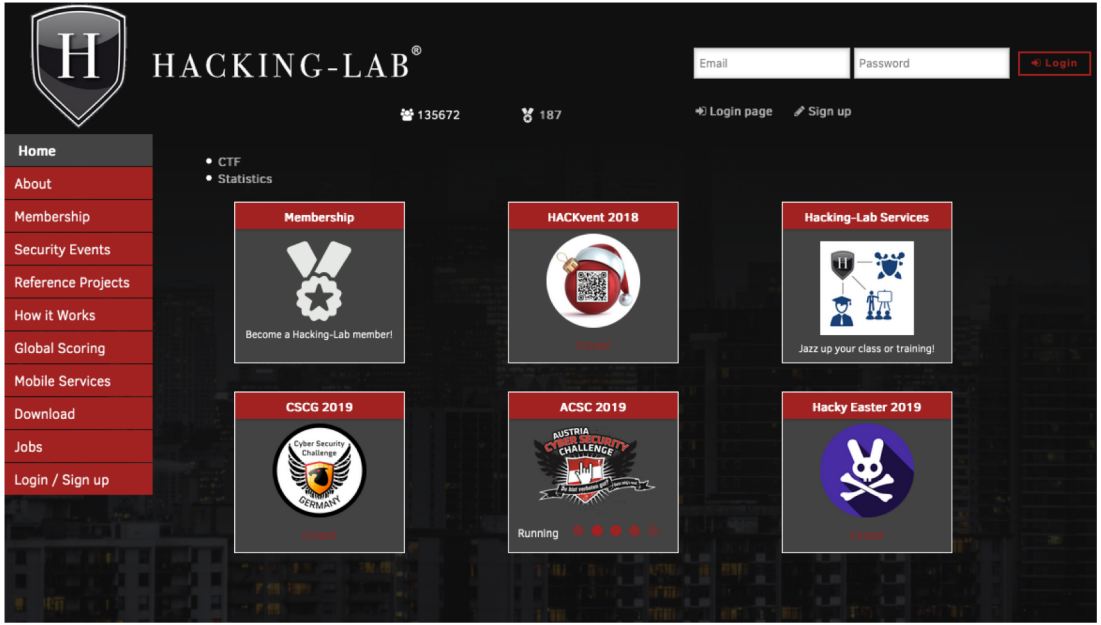
SWITCH

- Scenario #1: : An application encrypts **credit card numbers** in a database using **automatic database encryption**. However, this data is automatically decrypted when **retrieved**, allowing an **SQL injection flaw** to retrieve credit card numbers in clear text.
- Scenario #2: A site doesn't use or enforce **TLS** for all pages or supports **weak encryption**. An attacker **monitors network traffic** (e.g. at an insecure wireless network), **downgrades** connections from **HTTPS to HTTP**, intercepts requests, and steals the user's session cookie. The attacker then **replays** this cookie and hijacks the user's (authenticated) session, accessing or modifying the **user's private data**. Instead of the above they could alter all transported data, e.g. the recipient of a money transfer.
- Scenario #3: The password **database** uses **unsalted** or **simple hashes** to store everyone's passwords. A file upload flaw allows an attacker to **retrieve** the **password database**. All the unsalted hashes can be exposed with a **rainbow table** of pre **calculated hashes**. Hashes generated by simple or fast hash functions may be cracked by GPUs, even if they were salted.

A3:2017 Sensitive Data Exposure – Prevention

- **Classify** data processed, stored, or transmitted by an application.
- **Apply controls** as per the **classification**.
- **Don’t store sensitive data unnecessarily**. Discard it as soon as possible. Data that is not retained cannot be stolen.
- **Make sure to encrypt all sensitive data at rest**.
- Ensure up to date and **strong standard algorithms**
- **Encrypt** all **data** in **transit** with **secure protocols**
- **Disable caching** for **responses** that contain **sensitive data**.
- Store passwords using strong adaptive and **salted hashing functions**
- **Verify independently** the effectiveness of configuration and settings.

Further info and practices



https://www.hacking-lab.com/about/

What is Hacking-Lab?
Hacking-Lab is an online ethical hacking, computer network and security challenge platform, dedicated to finding and educating cyber security talents. … Hacking-Labs' goal is to raise awareness towards increased education and ethics in information security through a series of cyber competitions that encompass forensics, cryptography, reverse-engineering, ethical hacking and defense. One key initiative for Hacking-Lab is to foster an environment that creates cyber protection through education.

Threat Actors

- **Government Sponsored**: Well funded and often build **sophisticated, targeted attacks**. They are typically motivated by **political, economic, technical, and military agendas**.
- **Organized Crime**: Most often, these cybercriminals engage in **mass attacks** driven by **profits**. Typically looking for social security numbers, health records, credit cards, and banking information.
- **Hacktivists**: These attackers have a **political agenda** and create **high-profile attacks**
- **Insider Threat**: Insider attackers are typically **disgruntled employees** or ex-employees looking for **revenge** or some type of financial gain.
- **Opportunistic**: These attackers are usually **script kiddies** driven by the desire for **notoriety**
- **Internal User Error**: Users making **mistakes** with configurations which may bring down **critical resources** such as **firewalls**, routers and servers causing wide-spread or departmental company outages.

Threat Actors

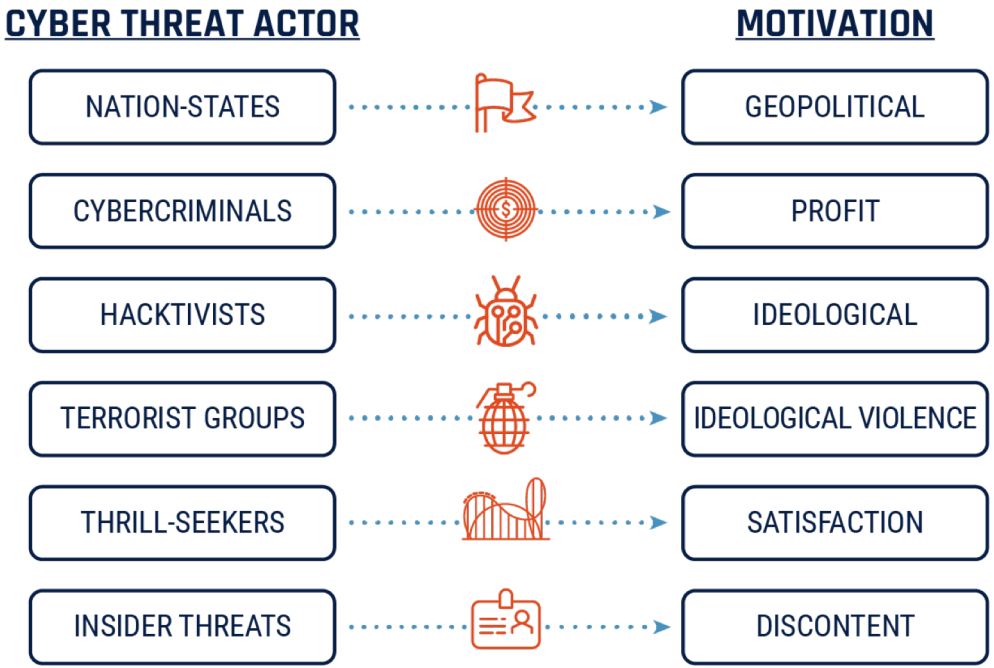
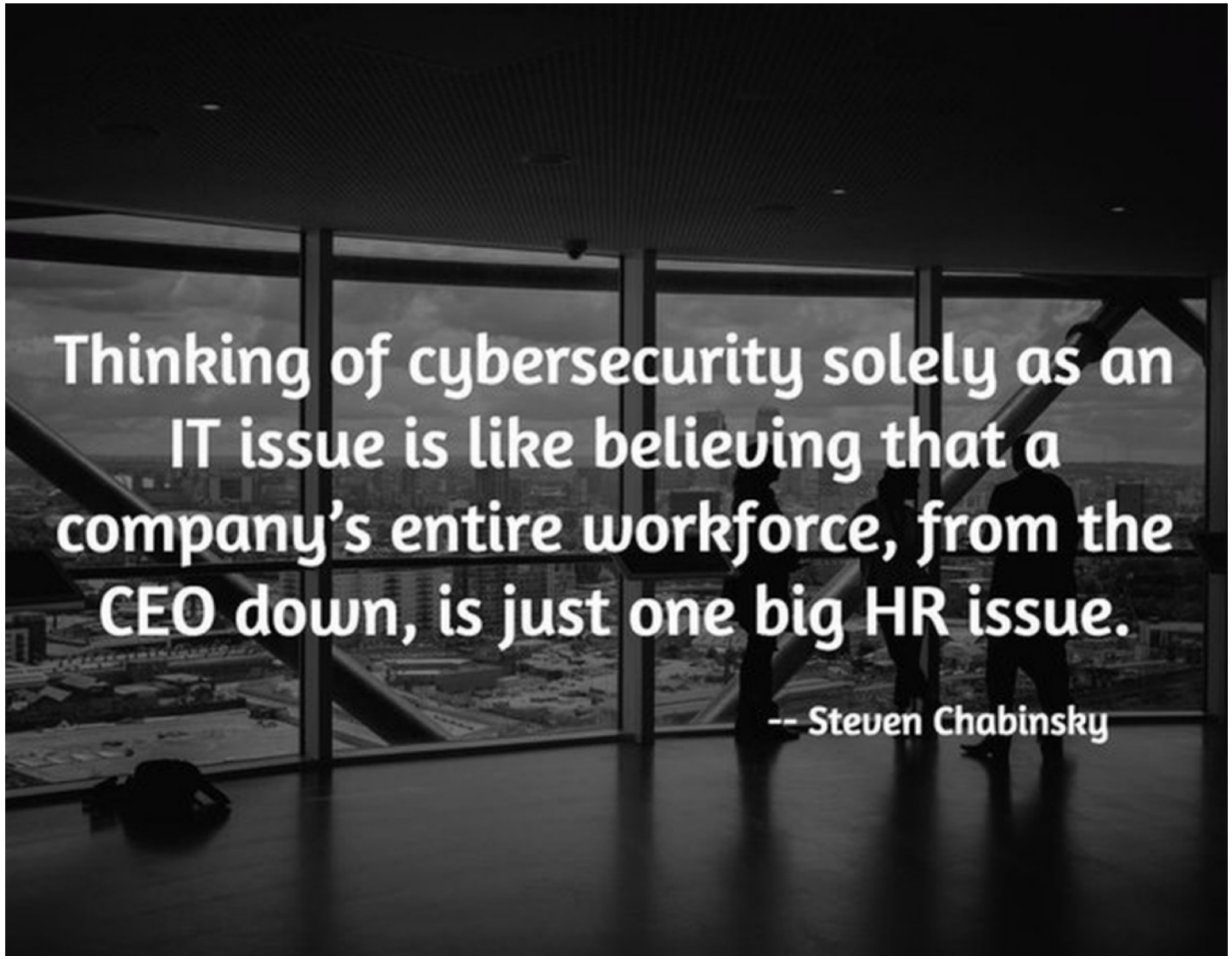


Image Source: https://cyber.gc.ca/sites/default/files/inline-images/motivations-e.png


Thinking of cybersecurity solely as an IT issue is like believing that a company's entire workforce, from the CEO down, is just one big HR issue.
-- Steven Chabinsky

Secure your Environment

- Security is a Process not just an Antivirus
- Awareness is a Key Component
- Harden your System
- Monitor your System
- Keep your Systems Up to Date

Problem with Security for Develloppers

Developer

Project Leader

Sponsor

Business Developer

Awareness

According to Swiss Study:

“More than half of the participants thought they were well informed about how to protect themselves against attacks from the Internet.”

https://ictswitzerland.ch/en/publications/studies/security-on-the-internet/

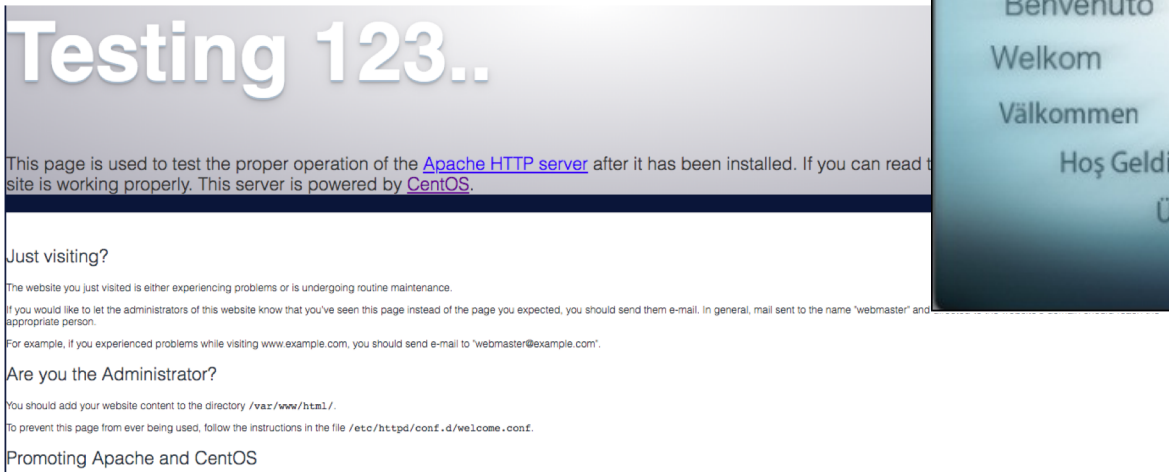
Awareness

- Let People think about Security
- Blog Posts and Campaigns
- Internal Training
- Ongoing Task to build Security Mindset

Hardening

- Most Software not Hardened by default
- Security vs. User-Friendly
- Check Guides from Vendor
- Deep Understanding required

Default Pages



Monitoring your System

- Finding abnormal or malicious Behaviour
- Hard Work to find good Baselines
- Use SIEM and/or Log Management Tools
- Only Monitor when Processes are in Place

Vulnerability and Patch Management

Question:

What Software do you use?


IT'S EASIER TO FIND
YOUR STUFF HERE
THAN HERE.

Vulnerability Management Topics

- Software Inventory
- CVE / CVSS / SCAP
- Vulnerability Scanner (Nessus)
- Penetration Testing / External Scans
- Zero Day Exploits

Types of Vulnerabilities

- DoS
- Code Execution
- Overflow
- Memory Corruption
- Sql Injection (OWASP)
- XSS (OWASP)
- Directory Traversal
- Http Response Splitting
- Bypass something
- Gain Information
- Gain Privileges
- CSRF
- File Inclusion

Types of Vulnerabilities

Security Vulnerabilities Published In 2019

2019 : January February March April May CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-1010260	284		Exec Code	2019-04-02	2019-04-04	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Using ktlint to download and execute custom rulesets can result in arbitrary code execution as the served jars can be compromised by a MITM. This attack is exploitable via Man in the Middle of the HTTP connection to the artifact servers. This vulnerability appears to have been fixed in 0.30.0 and later; after commit 5e547b287d6c260d328a2cb658dbe6b7a7ff2261.														
2	CVE-2019-1010258	119		Overflow Mem. Corr.	2019-05-15	2019-05-16	4.3	None	Remote	Medium	Not required	None	None	Partial
nanosvg library nanosvg after commit c1f6e209c16b18b46aa9f45d7e619acf42c29726 is affected by: Buffer Overflow. The impact is: Memory corruption leading to at least DoS. More severe impact vectors need more investigation. The component is: it's part of a svg processing library. function nsvg__parseColorRGB in src/nanosvg.h / line 1227. The attack vector is: It depends library usage. If input is passed from the network, then network connectivity is enough. Most likely an attack will require opening a specially crafted .svg file.														
3	CVE-2019-1010257	200		+Info	2019-03-27	2019-03-28	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
An Information Disclosure / Data Modification issue exists in article2pdf_getfile.php in the article2pdf Wordpress plugin 0.24, 0.25, 0.26, 0.27. A URL can be constructed which allows overriding the PDF file's path leading to any PDF whose path is known and which is readable to the web server can be downloaded. The file will be deleted after download if the web server has permission to do so. For PHP versions before 5.3, any file can be read by null terminating the string left of the file extension.														
4	CVE-2019-1003099	275			2019-04-04	2019-05-07	4.0	None	Remote	Low	Single system	None	Partial	None
A missing permission check in Jenkins openid Plugin in the OpenIdSsoSecurityRealm.DescriptorImpl#doValidate form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server.														
5	CVE-2019-1003098	352		CSRF	2019-04-04	2019-04-22	4.3	None	Remote	Medium	Not required	None	Partial	None
A cross-site request forgery vulnerability in Jenkins openid Plugin in the OpenIdSsoSecurityRealm.DescriptorImpl#doValidate form validation method allows attackers to initiate a connection to an attacker-specified server.														

CVE in Detail

- CVE-ID (Unique)
- Vulnerability Types
- Score
- Access (Remote, Local)
- Complexity

Task:

Search CVS Score > 7.5 for a Software of your choice
Present it afterwards in 30 seconds

Hints for Software to search

- Hadoop
- Elsticsearch
- Apache Spark
- MongoDB
- Redit
- Visual Studio Code
- Notepad++
- Microsoft Excel/Word/…
- Windows 10
- Cisco IOS

Some Ressources:

- https://cve.mitre.org
- *https://www.cvedetails.com*
- *https://nvd.nist.gov/vuln/*

Cisco Credential Vulnerability

- cisco-sa-20180307-cpcp
- cisco-sa-20180328-xesc
- cisco-sa-20180606-waas-snmp
- cisco-sa-20180718-policy-cm-default-psswrd

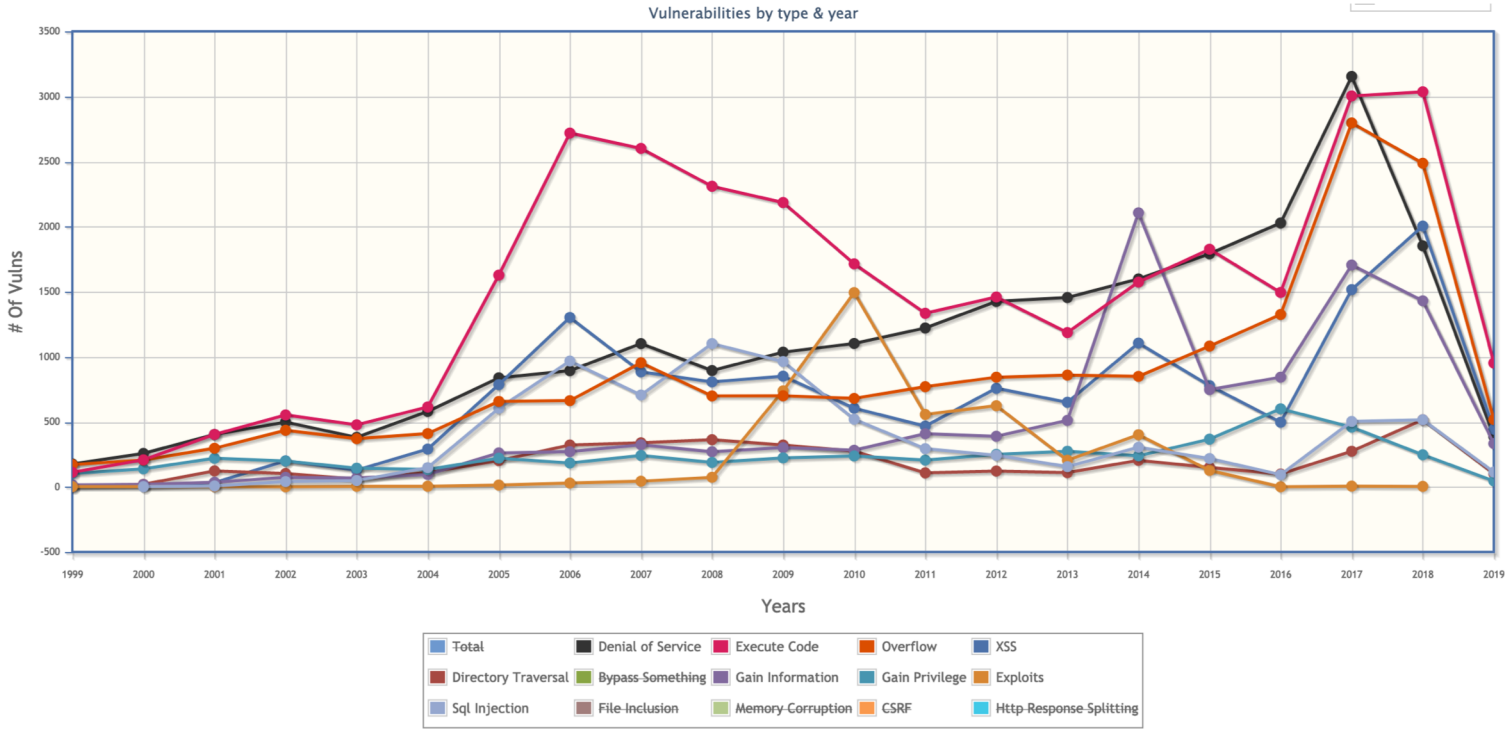
Score Calculation

- Base Score
- Temporal Score
- Environmental Score

Demo:

https://www.first.org/cvss/calculator/3.0

Found Vulnerabilities over Time



Source: https://www.cvedetails.com/vulnerabilities-by-types.php

Vulnerability Scanner

Demo

Patch Management

- Updates fixing bugs and vulnerabilities
- Automate as much as possible
- Updates can break things
- Different approach with Cloud

What needs to be Patched

- Hardware (Bios, Firmware, etc.)
- Virtualization Software (ESX, Hypervisor, LVM)
- Operating System
- Container
- Software / Framework

- Appliances
- Mobile Devices
- Out of Office Devices
- Don’t forget: Unmanaged Devices!

When Patch Management went Wrong

- Remote Desktop Environment
- After Test update one Server Crashed (In Test Week)
- Update was deployed everywhere
- Crashes followed on all Servers
- Removed Malicious update

Patch Management is a Process

- Define Schedules
- Prioritize Updates
- Test the Updates before complete Rollout
- Exceptions must be managed
- Have a Disaster Plan
- Make Someone responsible

Patch Management and Ressources

- Microsoft: WSUS
- Linux: UnattendUpgrades (Debian, Ubuntu)
- Redhat/Centos: Satellite

- Best Practice: Subscribe to Vendor Security Advisories

Vulnerability Management and Threats

- Keep your Room Clean (Basic Security)
- There are still open Doors (Zero Days Exploits)
- Keep your (Patch your System)

Best practices

- Stay updated - Subscribe to Security advisories
- Set passwords / Change standard passwords
- Use a password manager
- Secure/Harden your systems
- Run external scans

What is a ISMS?

- Information Security Management System
- A set of policies and procedures for systematically managing an organization's sensitive data
- Goal: Tominimize risk and ensure business continuity by pro-actively limiting the impact of a security breach

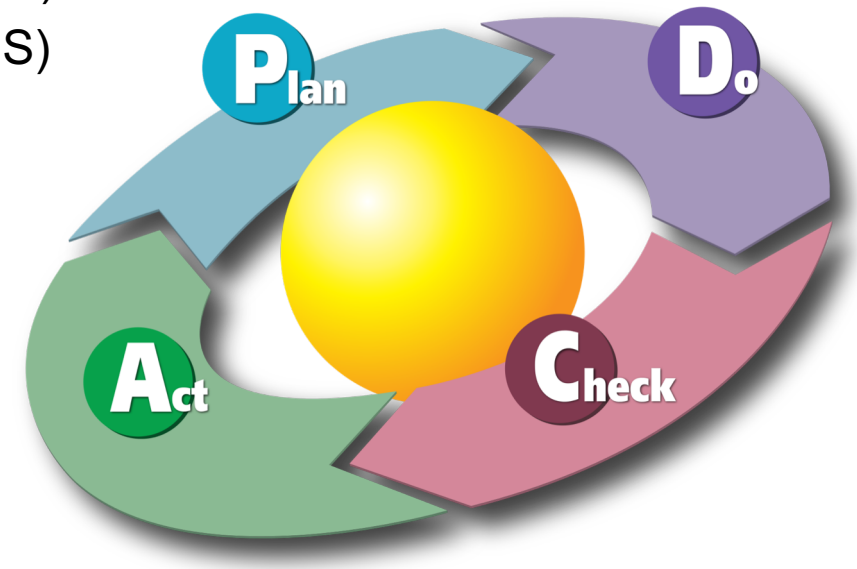
What is a ISMS?

- **I**nformation **S**ecurity **M**anagement **S**ystem
- A **set** of **policies** and **procedures** (“**controls**”) for **systematically** managing an organization's sensitive data.
- Goal: To **minimize risk** and **ensure business continuity** by pro-actively limiting the impact of a security breach
- An established **ISMS governs** the policies, procedures, processes, and workflows that are chosen to help protect an organization’s data security
- The organisation governs the policies with the **PDCA** (Plan, Do, Check, Act) **cycle**, regularly revisiting the procedures and adjusting them as needed

The PDCA cycle

- Plan (establishing the ISMS)
- Do (implementing and workings of the ISMS)
- Check (monitoring and review of the ISMS)
- Act (update and improvement of the ISMS)

https://en.wikipedia.org/wiki/ISO/IEC_27001



Standards / Risks

- ISO 27000 family of standards: ISMS Family $$$
  - https://www.iso.org/isoiec-27001-information-security.html
- ISO 31000 Risk management $$$
  - https://www.iso.org/iso-31000-risk-management.html
- BSI Grundschutz, Free
  - https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzDownloads/itgrundschutzDownloads_node.html

Standards / Risks

- “BSI Grundschutz”
  - **Threats (“Elementare Gefährdungen”)**

    As an example: “G 0.39 Schadprogramme” and “G 0.42 Social Engineering”
  - Modules (“Bausteine”)

    Process and System Modules

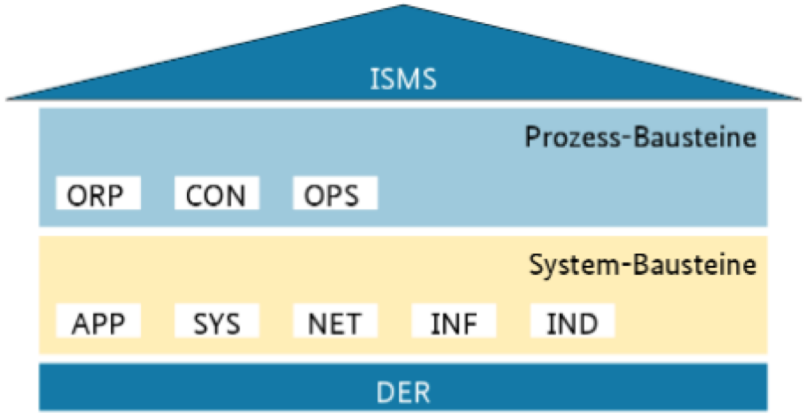


Image Source: “IT-Grundschutz-Kompendium: Stand Februar 2019”

How to React to a Security Incident

- Contact the right person within your organisation
  - CISO
  - Security Officer, SOC, CERT
  - IT department
  - CEO, Marketing / Communication
- Get external support if necessary
  - Incident Response Specialists, Forensic Experts
- Report the Security Incident
  - NREN organisations: SWITCH-CERT (https://www.switch.ch/security/contact/)
  - Melani (https://www.govcert.admin.ch/report/)
- Press charges (against unknown)
  - https://www.kkpks.ch/de/organisation/polizeikorps

How to React to a Security Incident

Report an incident to MELANI

If you want to report an IT security incident to MELANI, please use the following contact form:

- MELANI Reporting Form

Point of contact for CERTs and CSIRTs

As GovCERT.ch is the technical team of MELANI, the following email address can be considered as point of contact for FIRST members and other CERTs/CSIRTs. Please also direct any inquieries or reports regarding critical IT infrastructure in Switzerland to this email address. If you wish to communicate through a secure channel, please use our PGP key (download: 0x61624749) or SMIME certificate (download: govcert.crt).

Report an incident: incidents[at]govcert{dot}ch

Report a phishing site or phishing email

If you want to report a phishing site or phishing email, you can report them to antiphishing.ch:

- antiphishing.ch

Report a crime

If you wish to report a crime, please direct your request to the Cybercrime Coordinate Unit (CYCO), using the following contact form:

- CYCO Complaints Form

Point of Contact

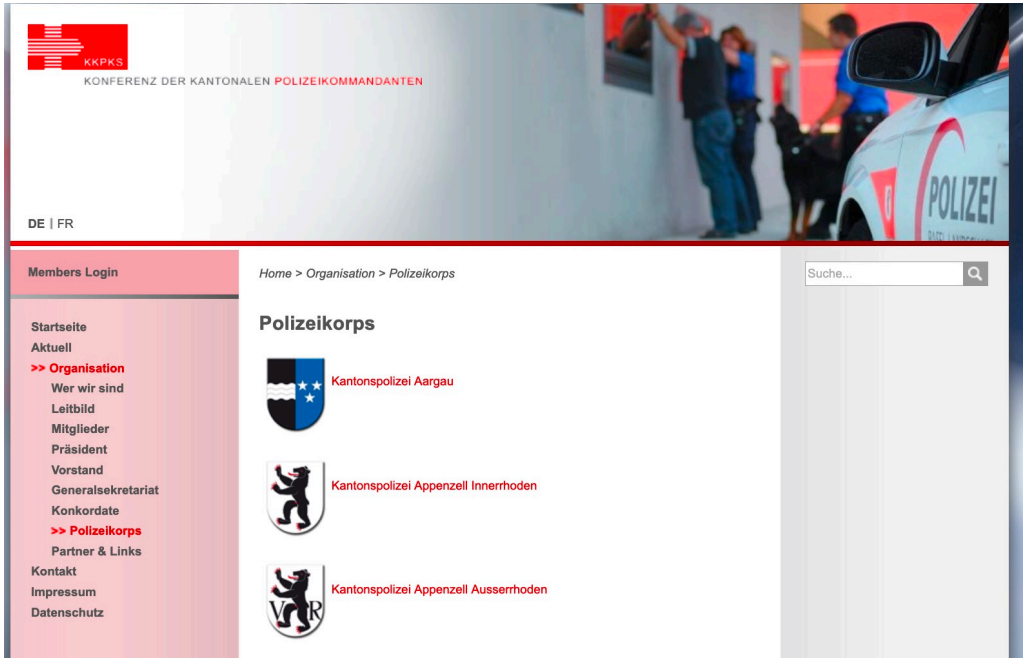
Report an incident to MELANI
Report a crime to CYCO
Report phishing
GovCERT.ch PGP-Key
GovCERT.ch SMIME

Reporting addresses

Report an incident:
incidents[at]govcert{dot}ch

General inquiries:
outreach[at]govcert{dot}ch

How to React to a Security Incident



https://www.kkpks.ch/de/organisation/polizeikorps

References

- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project
- https://www.entrustdatacard.com/knowledgebase/what-are-the-ssl-tls-certificate-assurance-levels
- https://en.wikipedia.org/wiki/Root_certificate#/media/File:Chain_of_trust.svg
- https://www.dynadot.com/community/help/question/what-is-punycode
- https://en.wikipedia.org/wiki/Stuxnet
- https://www.varonis.com/blog/advanced-persistent-threat/
- https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
- https://www.trendmicro.com/vinfo/us/security/definition/whale-phishing
- https://www.tbs-certificates.co.uk/FAQ/en/204.html
- https://www.cherwell.com/library/blog/what-is-an-information-management-security-system/
- https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one
- https://whatis.techtarget.com/definition/information-security-management-system-ISMS
- https://www.fortinet.com/blog/industry-trends/threat-intelligence-understanding-your-threat-actors-101-part-1-of-3.html
- https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

SWITCH

Working for a better digital world