AMable

Guide to Authentication and Data Security

Guide to Authentication and Security

Your data is your value. From office documents to product models, from e-mails to messaging services - digital information is part of our life and business.

Each one of us transfers such digital data through networks that we do not know. Each one of us relies on applications that we did not develop ourselves. We need to trust the service providers and the network operators but we can take responsibility for access to data and sharing of data.

This guide sets the scene for "client" side measures, for what we can do to protect our data. AMable has developed this guide with a specific focus on SMEs. Our aim was to inform and empower you. Still, there might be some places where you might feel the need for support.

Talk to us. We are there to help.

Security

What happens out there?

Security breaches happen each day

Stolen passwords often enable access to multiple platforms

Data sharing and privacy are the challenges of the century

According to Entrepreneur, during the past year 40% of people have been hacked at least once. The survey was conducted by mobile identity company TeleSign, which polled 2,000 consumers in the U.S. / U.K.

Google's and UC Berkeley's report on data breaching most important findings

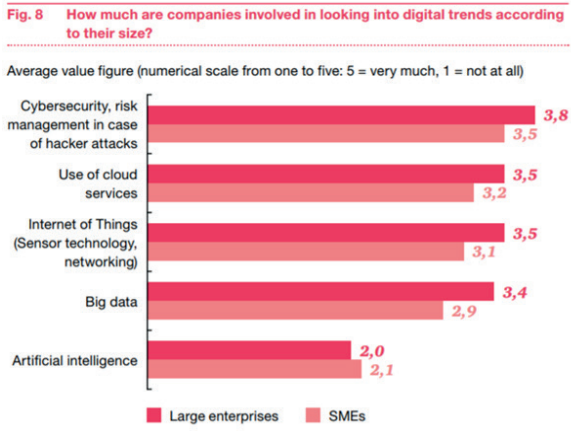
- Hacked passwords cause 81% of data breaches and rising
- 788,000 potential victims of off-the-shelf keyloggers
- 12.4 million potential victims of phishing kits
- 1.9 billion user names and passwords exposed via data breaches
- 7–25% of stolen passwords would enable access to other platforms through password re-use

Study on the development of the new data economy in the Industrial Data Space (IDS)

In a study from 2018, PWC portrays the current mood among companies on the extent of shared data. It flags the requirements, attitudes and conditions which need to be met to enable secure and trustworthy sharing of data through IDS technology. Executives from 210 large

enterprises, small and medium-sized companies and institutions were asked to participate in this survey.

In so-called placement interviews spontaneous reactions were collected and validated through follow up interviews.



Data exchange as a first step towards data economy, 2018, https://www.internationaldataspaces.org/publications/data-exchange-as-a-first-step-towards-data-economy-a-pwc-study-2/

As a key result the study states that data exchange between companies is an essential feature of digitisation and data economy

- More than 80% of the companies believe that digitisation will have a strong influence on their company.
- Currently, three out of four companies already exchange data.
- 74% of the companies assume that the demand for data exchange will increase in the medium term.
- Digitisation strategies are noticeably fewer in SMEs than in large enterprises. The main trigger for digital strategies seems to be security aspects.

Branch: master SecLists / Passwords /

Create new file Find file History

kazkansouh refreshed and fixed couple issues with cirt credentials Latest commit 0080212 20 days ago

..		
Common-Credentials	find . -name '*_*' -exec rename 's/_/-/g' "{}" \;	10 months ago
Cracked-Hashes	Quick rename of files	2 years ago
Default-Credentials	Merge pull request #357 from govolution/patch-3	5 months ago
Honeypot-Captures	51k random creds obtained by running Heralding for two weeks in Sep/2019	5 months ago
Leaked-Databases	Better filenames	10 months ago
Malware	Close #291 - Fix encoding issues	10 months ago
Permutations	rename 's/_/-/g'	3 years ago
Software	Close #291 - Fix encoding issues	10 months ago
WiFi-WPA	Add "-" to split up words, moved files since PR accepted	2 years ago
Keyboard-Combinations.txt	Add "-" to split up words, moved files since PR accepted	2 years ago
Most-Popular-Letter-Passes.txt	Add "-" to split up words, moved files since PR accepted	2 years ago
PHP-Magic-Hashes.txt	Adding sha256 magic hash	8 months ago
README.md	removes exec. bits	13 months ago
SCRABBLE-hackerhouse.tgz	Add scrabble	7 months ago
UserPassCombo-Jay.txt	"Passwords/" Clean up	3 years ago
bt4-password.txt	Close #291 - Fix encoding issues	10 months ago
cirt-default-passwords.txt	refreshed and fixed couple issues with cirt credentials	20 days ago
clarkson-university-82.txt	Quick rename of files	2 years ago
darkc0de.txt	Close #291 - Fix encoding issues	10 months ago
darkweb2017-top10.txt	Add "-" to split up words, moved files since PR accepted	2 years ago
darkweb2017-top100.txt	Close #291 - Fix encoding issues	10 months ago
darkweb2017-top1000.txt	Close #291 - Fix encoding issues	10 months ago
darkweb2017-top10000.txt	Close #291 - Fix encoding issues	10 months ago
der-postillon.txt	Add worlds-safest-password list by Der Postillon	11 months ago
dutch_wordlist	Added dutchwordlist	5 months ago
mssql-passwords-nansh0u-guardic...	Add MSSQL from guardicore: labs_campaigns-Nansh0u	9 months ago
openwall.net-all.txt	Close #291 - Fix encoding issues	10 months ago
probable-v2-top12000.txt	Add "-" to split up words, moved files since PR accepted	2 years ago
probable-v2-top1575.txt	Add "-" to split up words, moved files since PR accepted	2 years ago
probable-v2-top207.txt	Add "-" to split up words, moved files since PR accepted	2 years ago
richelieu-french-top20000.txt	Add richelieu	8 months ago
richelieu-french-top5000.txt	Add richelieu	8 months ago
stupid-ones-in-production.txt	Create stupid-ones-in-production.txt	7 months ago

- Data exchange is the basis for added-value processes today. Regular or comprehensive data exchange lies within 63% of companies.
- Awareness of cross-industry data exchange seems to be present in companies – more than 40% of the companies are considering this at a strategic level.
- 62% of data exchange is done with companies other than customers and suppliers, 15% of which is with direct competitors.

Securing Access

Authentication plays a key role when you allow a person or a software to access data. Solution providers increasingly implement rules to ensure a certain level of complexity for passwords. But still, the selection of a strong password relies on the user.

Strong Passwords

Use a strong password

A strong password does not contain

- personal information such as birth data, address or name of the company or friends
- consecutive or repeating numbers such as "1234" or "666"
- words from the dictionary such as "house", "car"

Store your passwords with safe applications in a safe environment

A strong password needs

- mixed elements from numbers, capital/small characters, special characters
- a certain length that achieves the required degree of complexity

Applications that calculate the complexity of passwords are widespread. Some of these are even offered as a service on the web. However, sending a sensitive password to an unknown website might not be the brightest idea.

Complex password can best be saved in password safes. These applications typically document the context of the password and allow automatic retrieval and even automatic transfer when needed. Most of these applications also calculate the complexity of the password or generate complex passwords (e.g. KeePass).

The only risk with password safes is, that they usually require one password to reveal all passwords of the respective user. This puts a strong emphasis onto this so-called master-password.

Multi Factor Authentication

Try to use multiple factors for authentication

Another option is the use of more than a single factor to authenticate yourself. Most business notebooks offer scanners for fingerprints or veins. With such a device, notebooks are able to provide the second factor that enhances authentication security, but only if they do not replace the need to type in a password.

Virtual private networks (VPN) often use a digital certificate as an additional authentication factor. Such certificates can be stored on plastic cards, similar to credit cards.

A digital certificate in combination with the users' password can be used for two-factor login to computer systems, applications or servers. Such a login is considered highly secure as the two factors come together from two physical channels and are joined only at the time when authentication is executed.

Encryption

In business or in private life, transfer of data takes place nearly all the time. Text messages from our smart phones, messages through the messenger services, or e-mails. But also during the visit of a web-site, a significant amount of data is transferred from the site to the visitor and vice versa.

Today, most messenger services provide an end-to-end encryption. This means, that data is encrypted at the sender's device

and de-crypted at the receiver's device. During transfer of that data, the so-called "man in the middle" only sees encrypted data, but not the content. This is even true for those web sites that offer the HTTPS protocol.

Now, secure transfer of data has three core benefits

- data that is intercepted on the transfer from sender to receiver cannot be used without de-crypting
- if data is encrypted against a registered certificate, only the registered receiver can de-crypt the data
- sender and receiver can agree on the complexity of the encryption, enabling dedicated security levels

The technical implementation of such secure transfer can be realised in two ways, encryption of the data file or encryption of the data transfer channel. Both approaches do not differ if data is transferred from the sender to the receiver directly. However, upload into a cloud storage space through an encrypted channel (e.g. HTTPS) does not fulfill the term "end-to-end" encryption.

Message Exchange

Consider how your data travels through the net

Encrypt sensitive data end-to-end

Secure message exchange is easy. For sending e-mails securely, you need to visit your mail client and install a digital certificate. For messenger services, you need to check the service description to see if it offers end-to-end encryption by default or if you need to configure it.

- Messages that are sent by e-mail should always use a secure transfer channel (SSL or TSL). This is a setting in the e-mail client program. Users must understand that the text in the message and that attachments can be used by anyone who receives the message.

- In case you send sensitive data, encrypt your e-mail. You need to get a certificate from a certification authority and you need the identity of the receiver (who also needs a certificate). Most e-mail clients allow you to configure "encryption" as the default option when composing your mail. So you do not forget to use it if you send your sensitive data.

File Transfer

Sending an encrypted file through an encrypted channel is better than attaching a week worth of work to a plain e-mail

Secure transfer of files is not so easy. There are plenty of transfer channels available, from e-mail attachment through file-transfer-protocol (FTP/SFTP) through cloud services (HTTPS with SSL/TLS) up to VPN connections. Users need to consider transit of data and its status after arrival.

- If you attach a file to an e-mail message and encrypt this message, then you should be safe that only the receiver will be able to de-crypt the file. Most systems however are limited to 10MB file size.
- If you transfer your sensitive data directly to the receiver through a secure channel with registered certificates (TLS), then you should be safe that the receiver will be the only one to have your file. However, the access control to the file then is up to the receiver.
- If you need to transfer data into a sharing platform or cloud service, and if your data is considered to be sensitive, then you should consider encrypting it before the transmission.

Resume

Authentication and security of data is not for free. But robust authentication and security of data is much cheaper than the value of your data.

AMable develops a dedicated AMable IDS Connector that allows you to transfer data from you to a receiver, both equipped with

registered certificates, both connected through a TLS link, both having a protocol of what has been transferred and if it was successful, with integrity check on both ends. Secure file transfer for AM related data end-to-end.

Talk to us. We support you.

Contact

projectoffice@amable.eu
www.amable.eu

Coordination

Fraunhofer Institute for Laser Technology ILT
c/o Ulrich Thombansen
+49/241/8906-320
ulrich.thombansen@ilt.fraunhofer.de

amable.eu

/company/amable-eu

@amable_eu

Channel: AMable

This project is co-funded by the European Union's Horizon 2020 research and innovation program under grant agreement 768775