Incident Response - Typische Fehler

CONOVA S-DAY 2021
Juni 2021

pwc

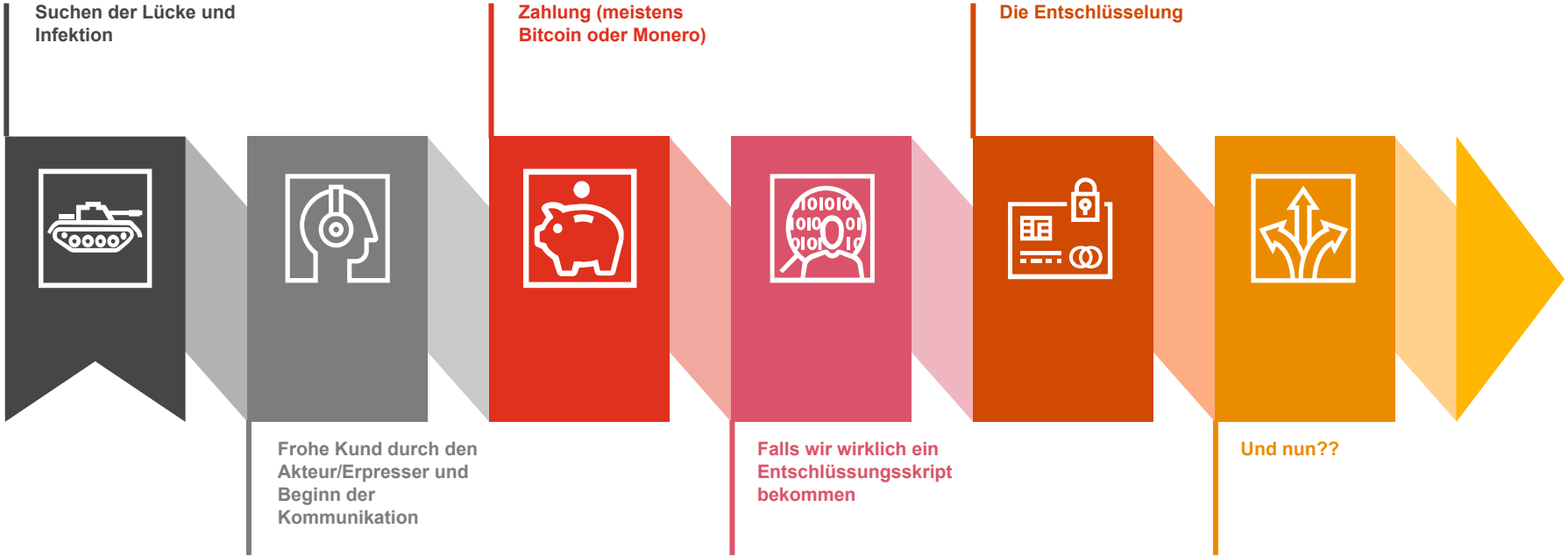

Ooops, your files ha
What Happened to My Con
Your important files are encrypted.
Many of your documents, photos, vi
accessible because they have been e
recover your files, but do not waste
our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can rec
not so enough time.
You can decrypt some of your files f
But if you want to decrypt all your fi
You only have 3 days to submit the p
Also, if you don't pay in 7 days, you
We will have free events for users w
How Do I Pay?
Payment is accepted in Bitcoin only.
Please check the current price of Bit
click <How to buy bitcoins>.
And send the correct amount to the
After your payment, click <Check Pa
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
bitcoin
ACCEPTED HERE
Send $300
12t9YDPgw

“ PANIK

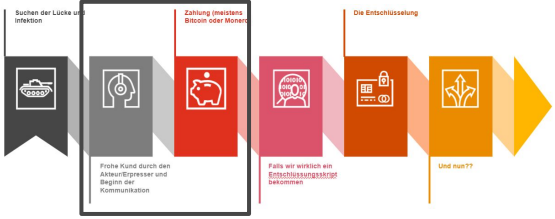
Handlungen im Affekt

“Wir haben alles im Blick

Was wäre wenn wir der Erpressung bei Ransomware folgen ...



Die Frohe Kund …
Kommunikation und Zahlung anonym …



##IMPORTANT_NOTICE## - Notepad

File Edit Format View Help

Greetings,
There was a serious security breach in your systems and this was detected during our scans.
We encrypt your data that you see important in your system by processing twice. As encryption is done as SHA256 and AES256, we would like to remind you that you can not restore your data with known da
process and / or make copies of them. Corruption of the original files may cause irretrievable damage to your data.
It is useful to know that random deletion techniques are used 3 times when you delete, you can not bring back deleted data by known methods.
These methods will only cause you to lose time.

If you wish, you can contact us via the following communication to resolve this issue.
Do not forget to add the specially generated code below when you want to reach it.

SITE_CODE:BF0EC0BB

datamoon@mail.com
data_lockerer@protonmail.com

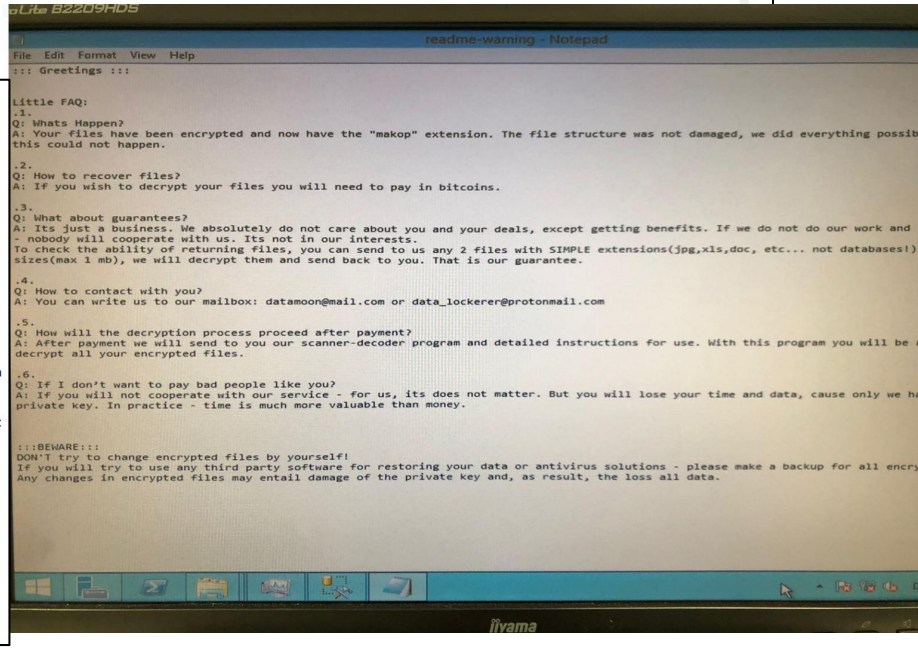
::: Greetings :::

Little FAQ:
.1.
Q: Whats Happen?
A: Your files have been encrypted. The file structure was not damaged, we did
everything possible so that this could not happen.

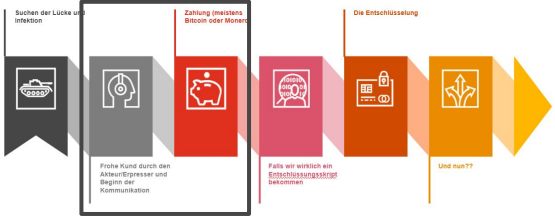
.2.
Q: How to recover files?
A: If you wish to decrypt your files you will need to pay in Monero(XMR) - this is one
of the types of cryptocurrency, you can get acquainted with it in more detail here:
https://www.getmonero.org/

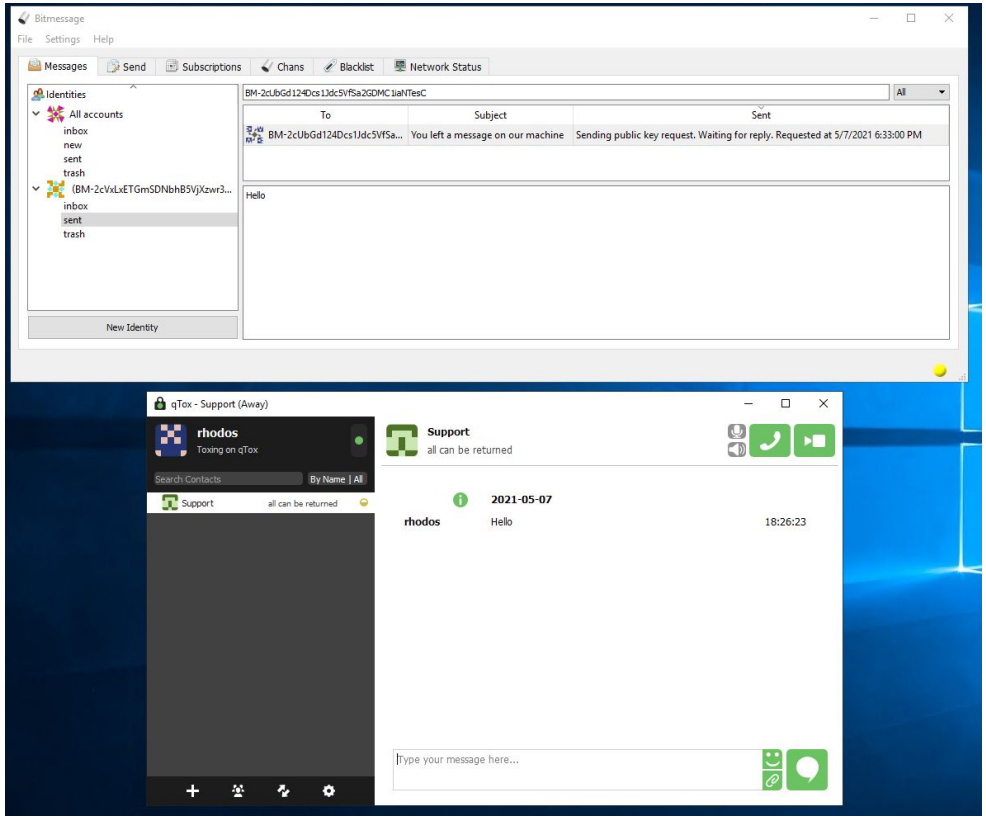
.3.
Q: What about guarantees?
A: Its just a business. We absolutely do not care about you and your deals, except
getting benefits. If we do not do our work and liabilities - nobody will cooperate with
us. Its not in our interests.
To check the ability of returning files, you can send to us any 2 files with SIMPLE
extensions(jpg,xls,doc, etc... not databases!) and low sizes(max 1 mb), we will decrypt
them and send back to you. That is our guarantee.

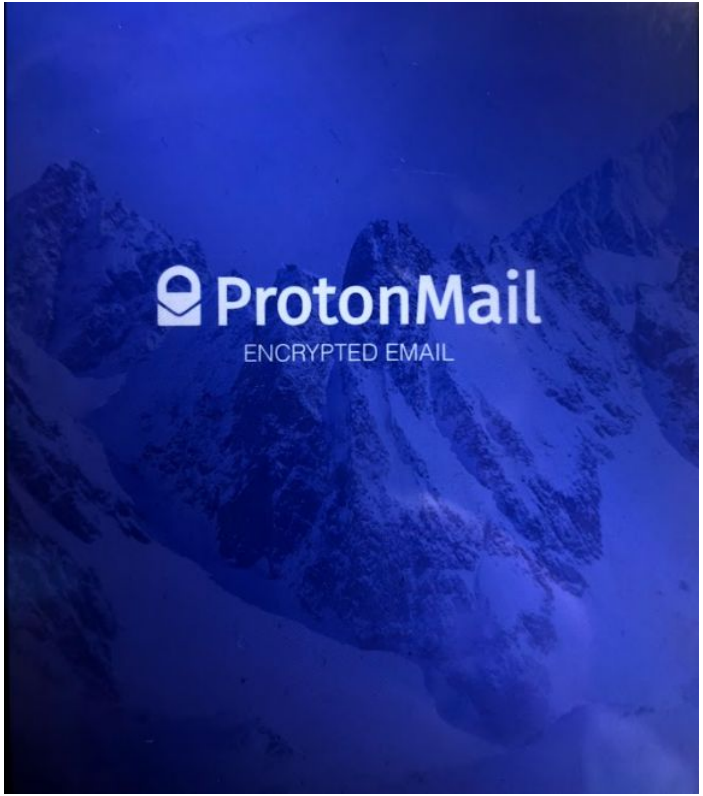
.4.
Q: How to contact with you?
A: Please, write us to our qTOX account:
7BDD546F7524089A930B12F793F4C1D1B4470A15A4CBA85AA0DA6D030AFE2E48B8799204F004
   You can learn about this way of communication and download it here:
https://qtox.github.io/
Or use Bitmessage and write to our address: BM-2cUbGd124Dcs1Jdc5VfSa2GDMC1iaNTesC
   You can learn about this way of communication and download it here:
https://wiki.bitmessage.org/ and here:
https://github.com/Bitmessage/PyBitmessage/releases/



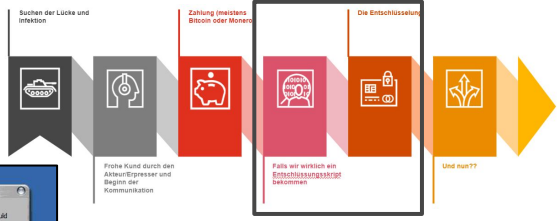
Die Frohe Kund …
Kommunikation und Zahlung anonym …

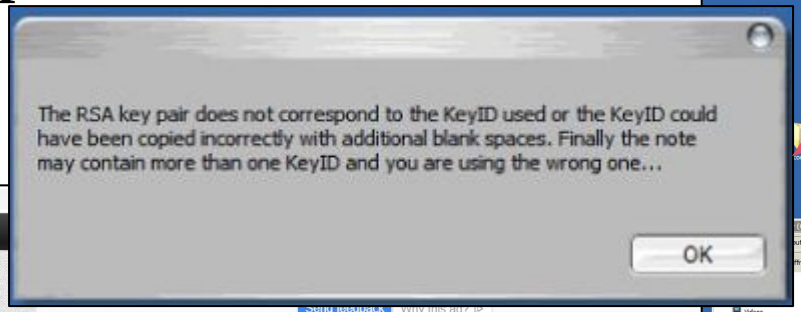


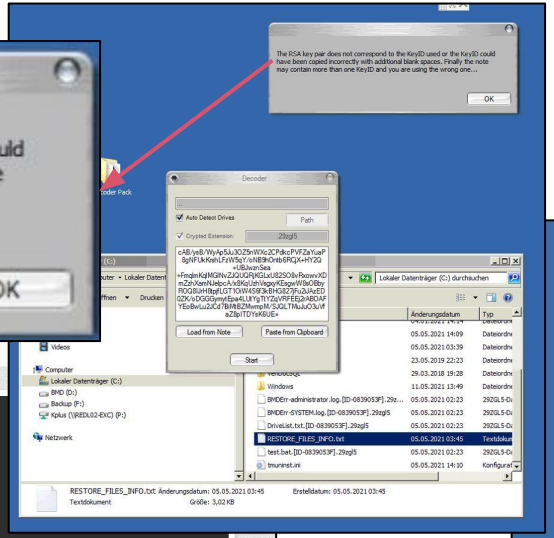


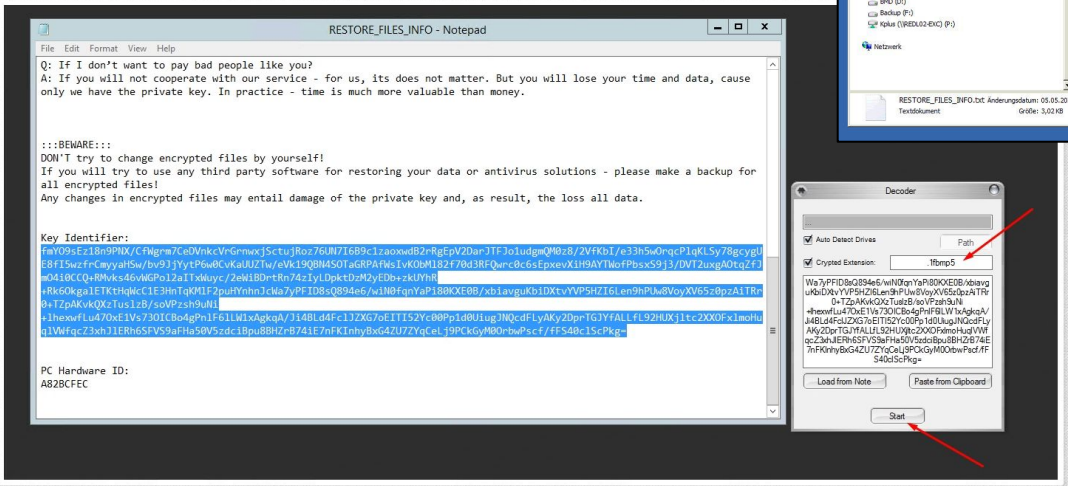


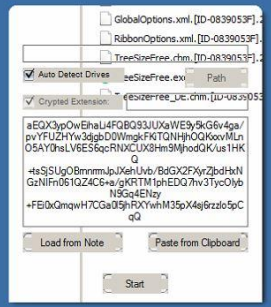
Falls wir wirklich ein Entschlüsselungs-skript bekommen

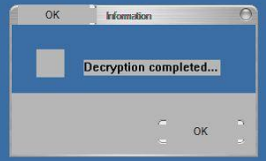




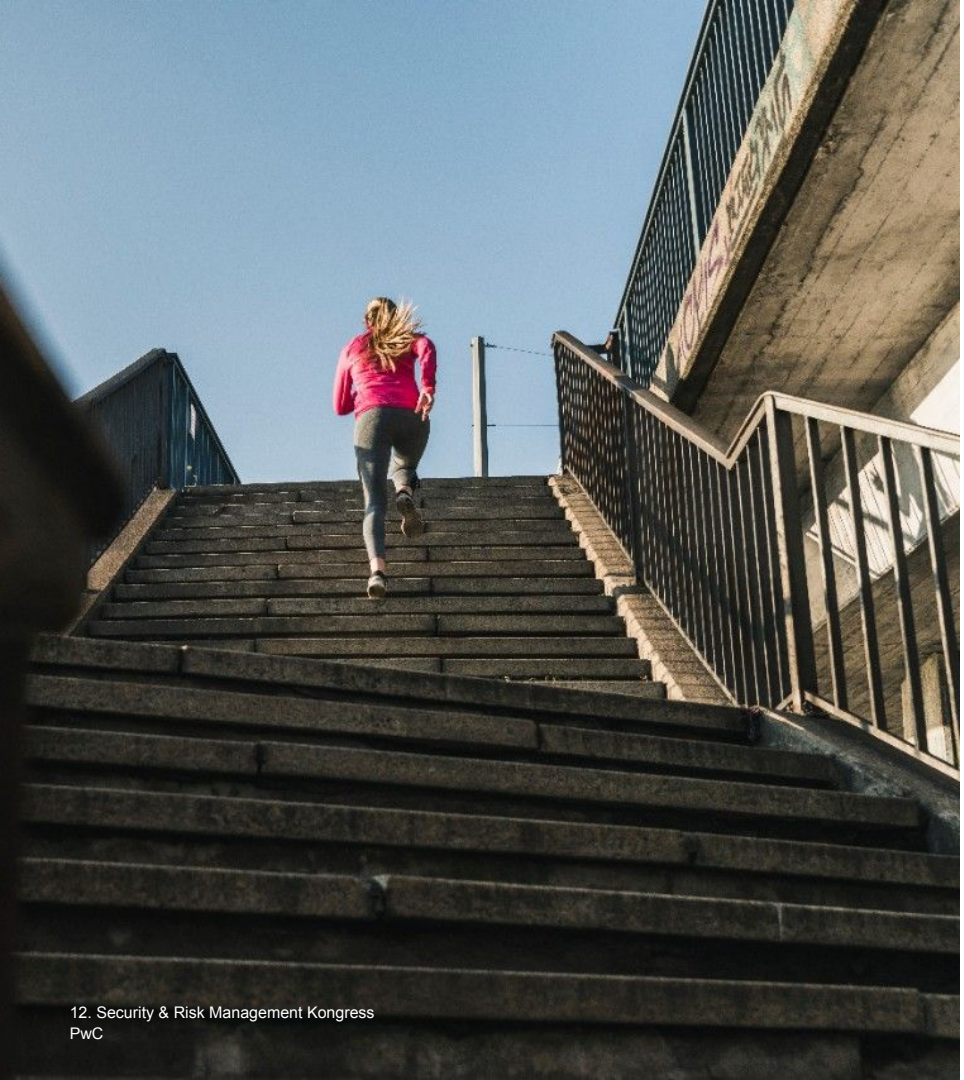






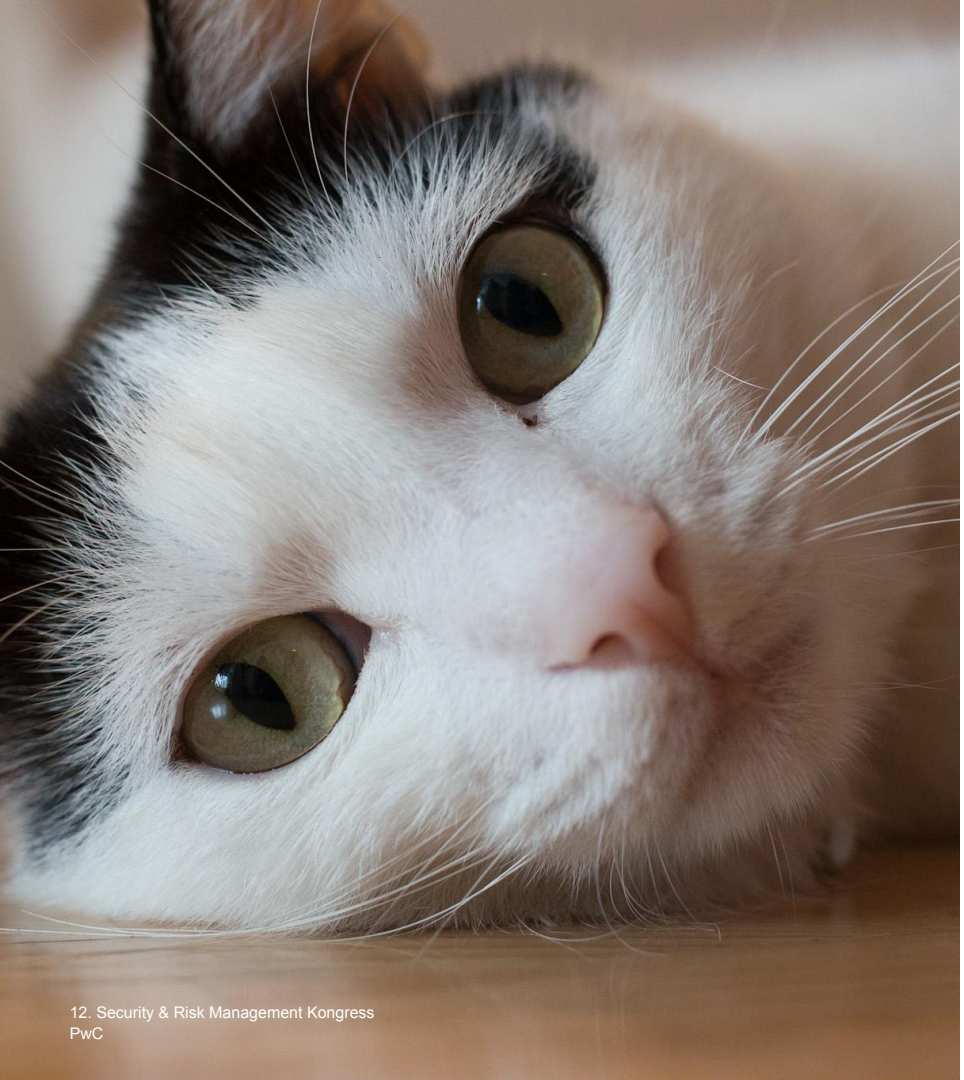


Mit Lightshot geschossen



“

Übungen? Sind nicht mehr im Budget.



Schrödinger’s Cyber Defense

Thank you

Erik Rusek
Senior Manager
Cybersecurity & Privacy
Tel.: +43 676 833775456
erik.rusek@pwc.com

Thomas Kastner
Manager
Cybersecurity & Privacy
Tel.: +43 676 833773231
thomas.k.kastner@pwc.com

pwc.at/cyber