glueckkanja gab

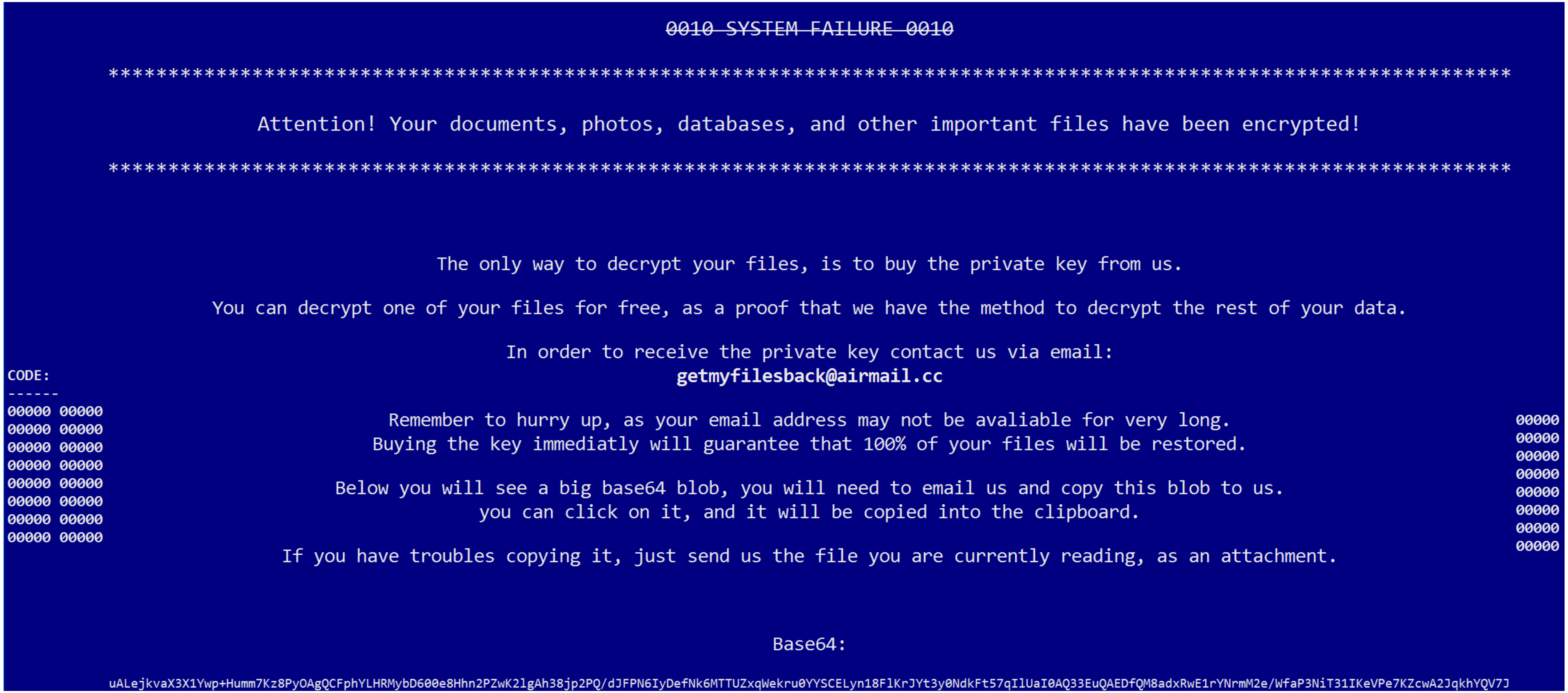
The Worst Case

How AzERE can support your
disaster recovery strategy
in case of a successful ransomware attack

RANSOMWARE ['ɹɛnsəmwɛːɐ̯]

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off.

Surprises @ work



~~0010 SYSTEM FAILURE 0010~~

****

Attention! Your documents, photos, databases, and other important files have been encrypted!

****

The only way to decrypt your files, is to buy the private key from us.

You can decrypt one of your files for free, as a proof that we have the method to decrypt the rest of your data.

In order to receive the private key contact us via email:
getmyfilesback@airmail.cc

Remember to hurry up, as your email address may not be avaliable for very long.
Buying the key immediatly will guarantee that 100% of your files will be restored.

Below you will see a big base64 blob, you will need to email us and copy this blob to us.
you can click on it, and it will be copied into the clipboard.

If you have troubles copying it, just send us the file you are currently reading, as an attachment.

```
CODE:
------
00000 00000
00000 00000
00000 00000
00000 00000
00000 00000
00000 00000
00000 00000
00000 00000
```

```
00000
00000
00000
00000
00000
00000
00000
00000
```

Base64:

uALejkvaX3X1Ywp+Humm7Kz8PyOAgQCFphYLHRMybD600e8Hhn2PZwK2lgAh38jp2PQ/dJFPN6IyDefNk6MTTUZxqWekru0YYSCELyn18FlKrJYt3y0NdkFt57qIlUaI0AQ33EuQAEDfQM8adxRwE1rYNrmM2e/WfaP3NiT31IKeVPe7KZcwA2JqkhYQV7J

Experiences from the field

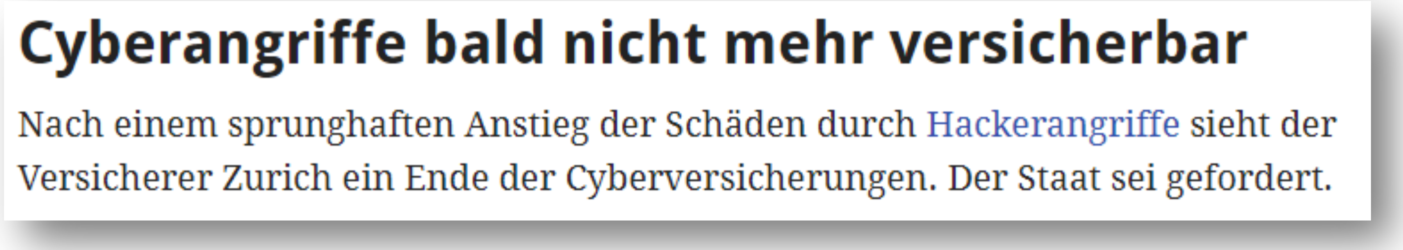
Digital Communication is broken

Missing trust in on existing infrastructure

Greenfield for AD Domain is almost impossible

Identities are starting point for restore
Domain Controller is the foundation for most (legacy) application

External parties delaying restore

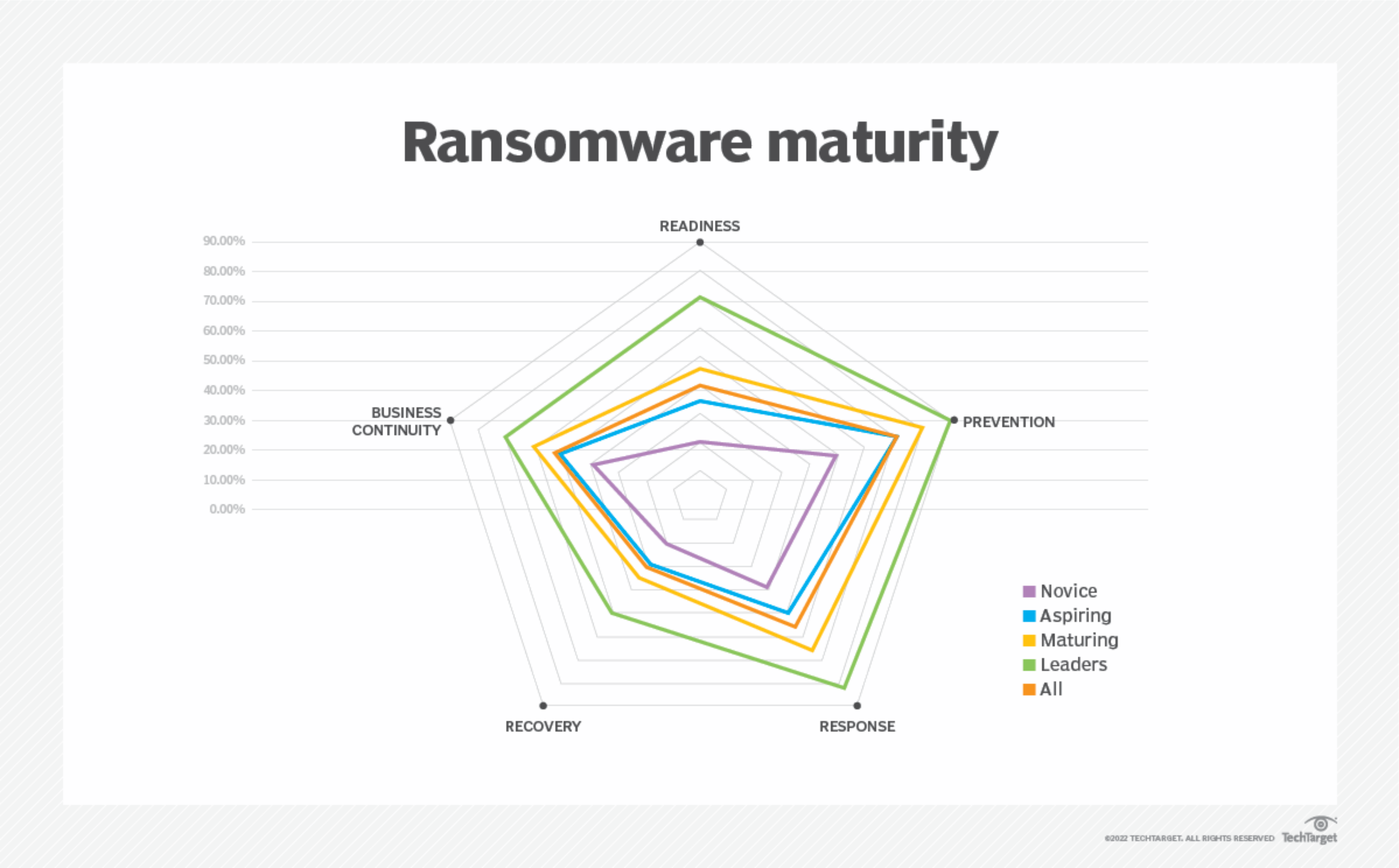


Cyberangriffe bald nicht mehr versicherbar

Nach einem sprunghaften Anstieg der Schäden durch Hackerangriffe sieht der Versicherer Zurich ein Ende der Cyberversicherungen. Der Staat sei gefordert.

Processes are not in place, time is running away

Experiences from the field



©2022 TECHTARGET. ALL RIGHTS RESERVED TechTarget glueckkanja gab

Introducing AzERE

Azure **E**mergency **R**esponse **E**nvironments

Goal of AzERE

- Design a solution that protects critical business services and withstands a **successful** ransomware attack.
- Critical business services consists of
  - Active Directory
  - Identities
  - Optional: A defined set of critical business applications
- After a successful ransomware attack, the RTO for the most critical services should be only a few days
- An automated process to provide a collaboration platform to a subset of users within the first hours after the attack.
- Strong focus on REGULAR fire testing
- The environment is built with 100% DevOps including Infrastructure as Code with terraform.

Non-goals of AzERE

- The solution is **not a backup replacement**.
- This solution is not a complete business continuity and disaster recovery (BCDR) strategy. AzERE can be a part of your BDCR strategy to quickly recover from a successful ransomware attack.
- Mail / Exchange is not considered as a critical business service. Even though email is critical in the day-to-day work, the importance of mail is the ability to receive and send **new** emails. Old and archived data can be restored later in time.