Europe Show

27 - 29 September 2021

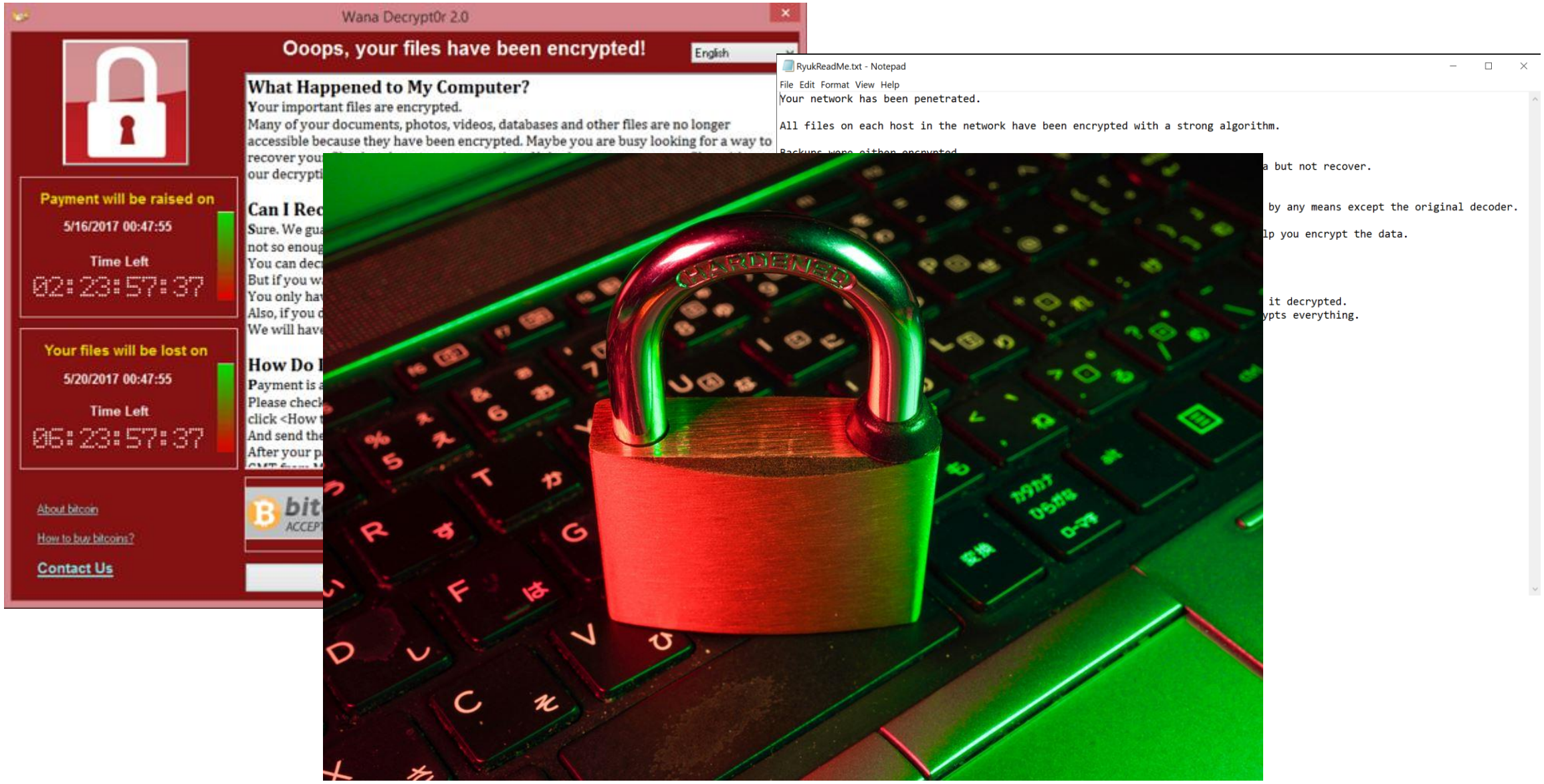
Getting a Grip on Data Breaches

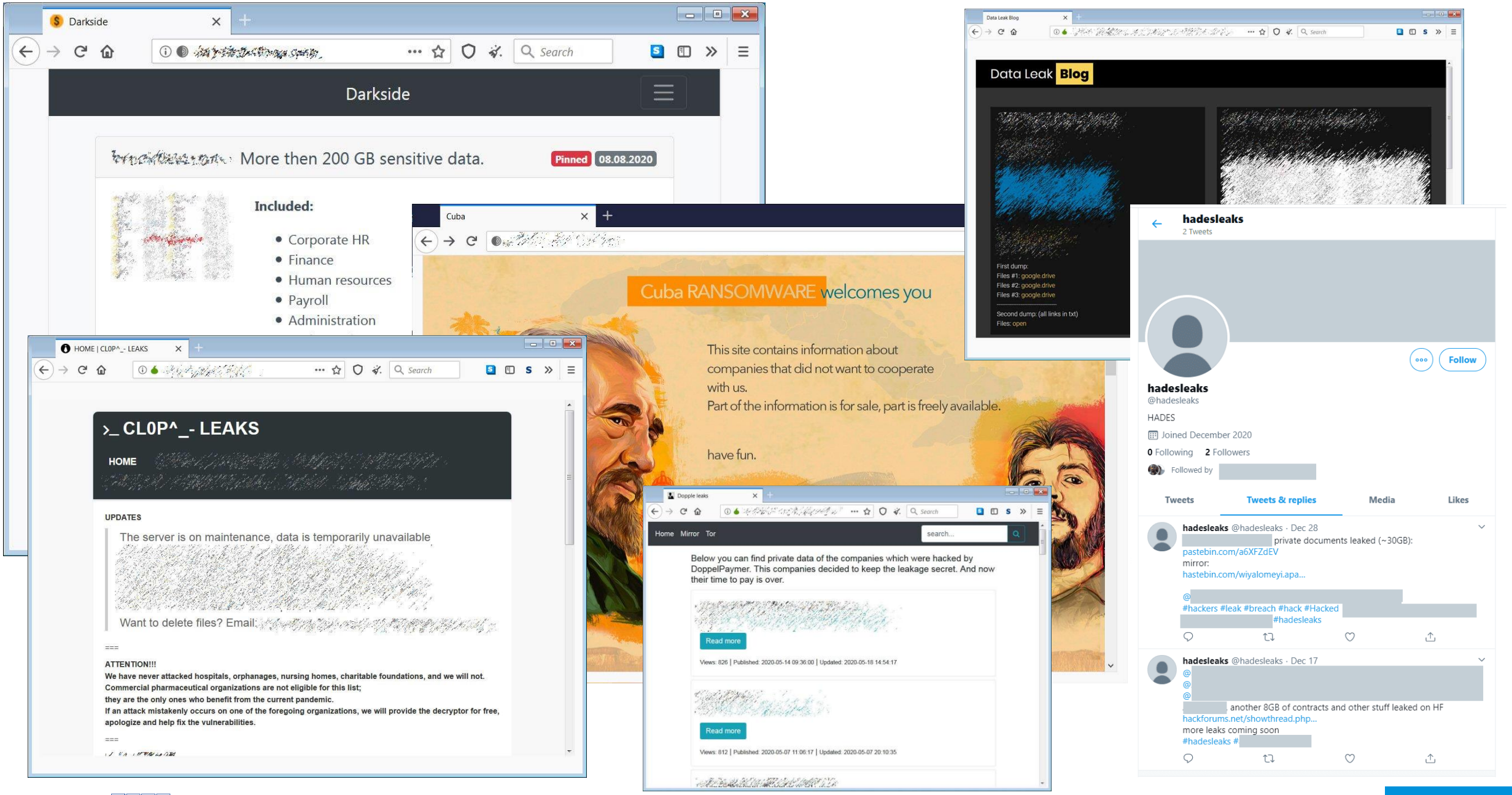
Ian Dashorst

Manager Forensic

KPMG

Getting a Grip on Data Breaches





Contents

01 Welcome

02 GDPR and data breaches

03 GDPR scan

04 Zero trust

05 Questions

GDPR and data breaches

Art. 33 – 34 GDPR (notification data breaches)	Publication: 2016
Guidelines EDPB, WP250	October 2017
Examples regarding Data Breach Notification, EDPB Guidelines 01/2021	Januari, 2021

The Basics

Guidelines EDPB, WP250

Definition of a data breach:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

Three breach types

Guidelines EDPB, WP250

Availability	Where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
Integrity	Where there is an unauthorised or accidental alteration of personal data.
Confidentiality	Where there is an unauthorised or accidental disclosure of, or access to, personal data.

Example case – Ransomware

- **Large international organisation**
- **Scattered IT landscape**
- **Servers in more than 50 countries**

Notification

Guidelines EDPB, WP250

Notification to the supervisory authority

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

Process

Obtain insight in the nature, size and period of the incident, including GDPR relevant domains.

Identify duration, extent and probability of data exfiltration through forensic investigation.

Reevaluate the risk of a data breach and the implications of the obtained insights.

Evaluate recovery and improvement measures.

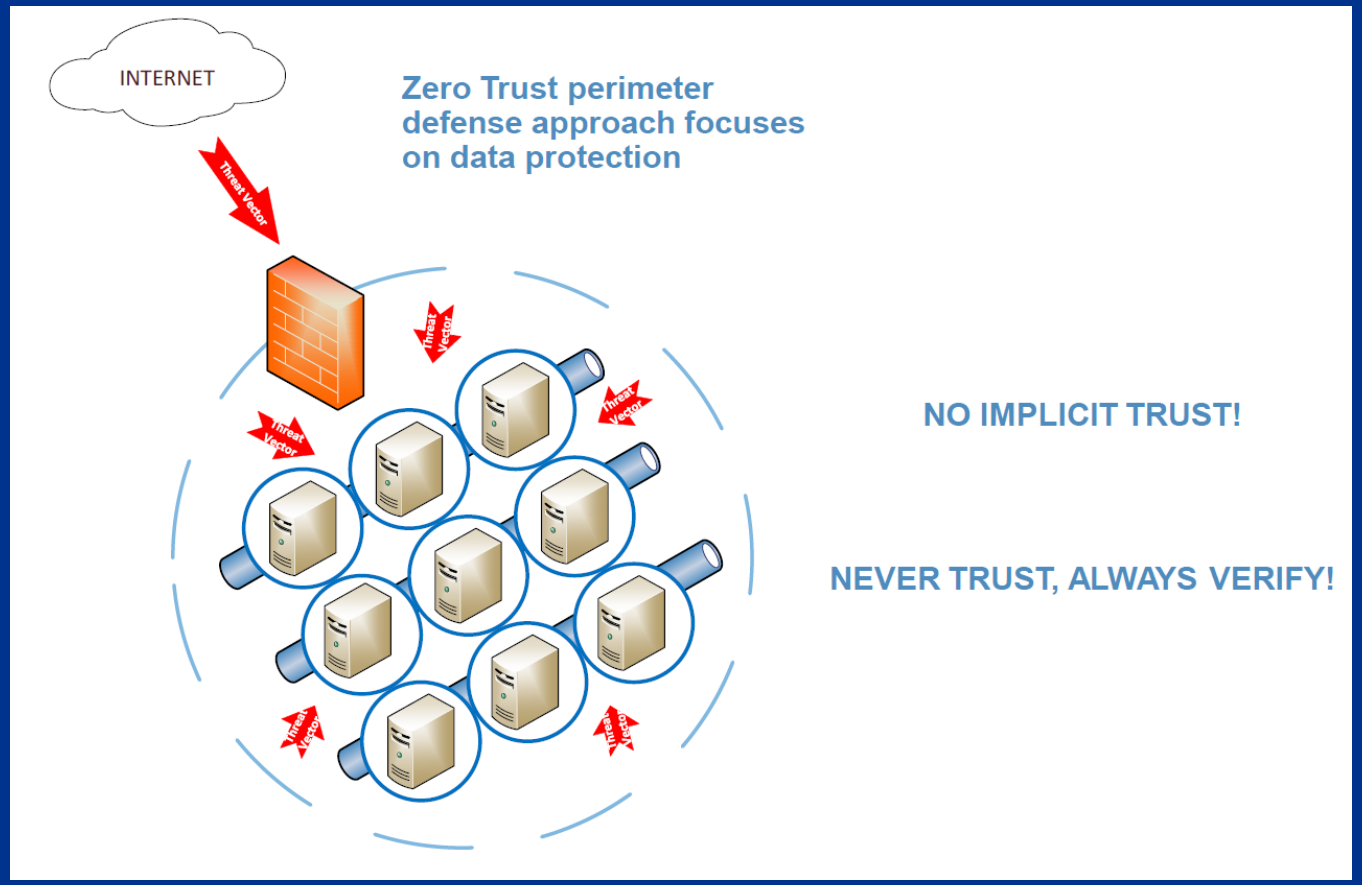
Consider regulatory requirements for reporting and notification

Example case – Phishing

- **An employee received PDF link**
- **Entered the credentials into a fake Microsoft login screen**
- **MFA was on the roadmap to be implemented for O365**
- **Two days later a phishing e-mail was sent from the account to 1,500 contacts within and outside the organization**

GDPR scan

Zero trust



Source: NIST National Cybersecurity Center of Excellence

Q&A

Thank you