Microsoft

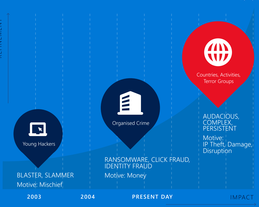
CYBERCRIME

DATA IS THE NEW GOLD

1. THE DEVELOPMENT OF CYBERCRIME

Cybercrime no longer just involves mischief caused by young hackers; nowadays it is big business.

Given that company data is used as the basis for a relationship of trust, it is crucial that this data is protected properly.



2. CURRENT RISKS

Cybercrime actively capitalises on these risks.

Of network attacks use weak or stolen login data

Of employees use unauthorised Software-as-a-Service (SaaS).

Of attacks come from unknown ransomware. Ransomware is a growing problem.

In 2015, 20% of Distributed Denial of Service (DDoS) attacks were on a scale of more than 50 Gb per second, which meant that sites and services were inaccessible.

In the context of the increasing threat, there are

4 STRIKING DEVELOPMENTS

from the CSBN 2016

Professional criminals are focusing on long-term, high-quality and advanced operations

Digital economic espionage by foreign intelligence services is putting the competitive position of the Netherlands under pressure

Ransomware is commonplace and has become even more advanced

Advertising networks do not yet have the capacity to deal with malvertising

3.

"Businesses and users are going to use technology only if they can trust it"

— Satya Nadella
CEO Microsoft

3. IMPACT EXTENDS FURTHER THAN JUST THE FINANCIAL EFFECTS

- Role of organised crime increasing all the time
- Disruption and danger to the basic infrastructure and systems
- Infringement of privacy
- Reduced innovation
- Diminishing trust

Of organisations believe they may have been the target of a cyber attack.

556 million

Victims of cybercrime per year

160 million

Data records compromised by the top 8 security violations in 2015

400 billion

Cyberattacks on companies costing 400 billion euros per year (damage)

140 +

average of 140+ days between the infiltration and detection of security violations

€ 3.000.000.000.000.000.000

(18 zeroes = trillion)

Estimated costs in terms of the economic value of the cybercrime industry in 2020

4. A REAL LIFE RANSOMWARE HIT

1. Digital assets (especially data) stolen from consumers and companies (made inaccessible with strong encryption)
2. Demand for victims to pay for a decoding key
3. Techniques to exert extreme pressure to force victims to pay
4. Anonymity is the top priority
5. Still relatively small amounts (up to now)

5. OUR VISION: PROTECT YOUR SME COMPANY

Continuous process and improvement cycle

1. PROTECT

- Protect your company on 4 levels:
- Create a good foundation based on your infrastructure
- Manage your corporate and personal devices
- Protect your apps and data and make sure there are extra security layers alongside passwords
- Protect your identity

2. DETECT

- Detect problems in good time by means of automatic analyses
- Proactively receive notifications and identify threats
- Data leaks are only discovered after an average of 140 days

3. REACT

- Quickly track down the source
- Take appropriate measures against infected devices, suspicious apps and unauthorised access
- Restore productivity with minimum disruption of work

6. OUR VISION OF DIGITAL TRANSFORMATION AND SECURITY

IMPORTANT **TECHNOLOGICAL TRENDS:**

- Augmented Reality
- Cloud
- Internet of Things (IoT)
- Virtual Reality
- Agile
- Quantum computing
- Machine learning
- Predictive analysis
- Blockchain

More information? Check https://www.microsoft.com/en-us/security

Microsoft