shaping tomorrow with you

FUJITSU

Protect & progress with cyber security in 2018

By 2020 there will be over 4 billion people online. The significant increase of cloud computing for business and personal use means there will be increased opportunities for cyber criminals in 2018.

Biggest Data Breaches of the 21st Century

- **143m** Equifax 2017
- **145m** eBay 2014
- **3b** Yahoo 2013

Cyber Security Eurobarometer

43% are concerned about the misuse of personal data

Over 5,5m cyber-attacks are thought to take place each year

42% are concerned about security around online payments

Jargon Buster

ATC – Advanced Threat Centre

BYOD – Bring Your Own Device

SOC – A Security Operations Centre

CTI – Cyber Threat Intelligence

SAO – Security Automation & Orchestration

Phishing – sending emails claiming to be reputable senders, encouraging recipients to provide sensitive data

Incident response – a planned method to address the aftermath of a security breach

Zero day – a cyber-attack for which developers have zero days to fix a problem that has potentially already been exploited by hackers.

GDPR – The Global Data Protection Regulation Act

GDPR - 25th May 2018

On the 25th May, data protection for businesses will become a legal requirement. GDPR forces organisations to review and enhance their data practices, putting strategies and policies in place to reduce risk of attacks.

Failure to comply with GDPR could result in a fine of 4% of your annual turnover or a fine of up to 20 million Euros

Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) can be defined in many different ways and it can simply be a threat feed. In most cases, that threat intelligence is providing guidance on 'protecting' using basic defences; i.e. patch management.

During 2018, it will be important to use CTI to provide an early warning system to customers and context to threats.

Petya

During last year's Petya outbreak, the malware used an SMB vulnerability for propagation that only needed patching.

Fujitsu provided a threat advisory on that patch to CTI customers 3 months before Petya spread.

SOCs must keep up with a wide range of cybercrime.

An advanced threat eco-system is required where human cyber skills are merged with security automation and orchestration.

SOCs will leverage AI and machine learning for effective security monitoring, freeing up valuable analyst time.

SOCs are responsible for harnessing cyber threat intelligence. Human analysts must combine with technical data collection platforms to provide actual threat insights.

Why Should You Use CTI

- Quick risk assessment
- Effective integration into existing tech
- Prioritisation of alerts & threats
- Reduced costs

Zero Day

A zero-day attack is a previously undetected vulnerability that has already been exploited by a hacker, leaving zero days for developers to fix the problem.

Nearly 1/3 of all cyber-attacks are zero-day exploits

How Can We Help?

- Identify
- Protect
- Defend
- Respond

- Information is the new currency, making data management, storage & access paramount for businesses.
- Fujitsu aim to transform SOCs into Advanced Threat Centres, to protect business' reputations with an intelligence-led approach.
- Fujitsu's cyber security business protects government departments, strengthening resilience as part of a globally-integrated security offering.

PalmSecure - As organisations search for more secure authentication methods for data access, physical access and general security, many are turning to biometrics

- Vein patterns are unique to individuals
- Contactless authentication is hygienic
- High level of accuracy and application versatility

385m

385 million personal email addresses were uncovered by Fujitsu from a Russian server including government agencies and banks.

Our Key Services:

- Predictive intelligent threat detection
- Trusted delivery
- Expert-led managed security services
- Global 24/7 monitoring & response

Visit the Secure Thinking website to find out more about keeping your business protected from cyber threats.

FUJITSU