HORNETSECURITY

Compliance Mastery

Intro to Pauline Brace, URM Consulting

HORNETSECURITY

INTRODUCTION

HORNETSECURITY

PAULINE BRACE

Senior Data Protection and
Information Security Consultant

pbrace@urmconsulting.com

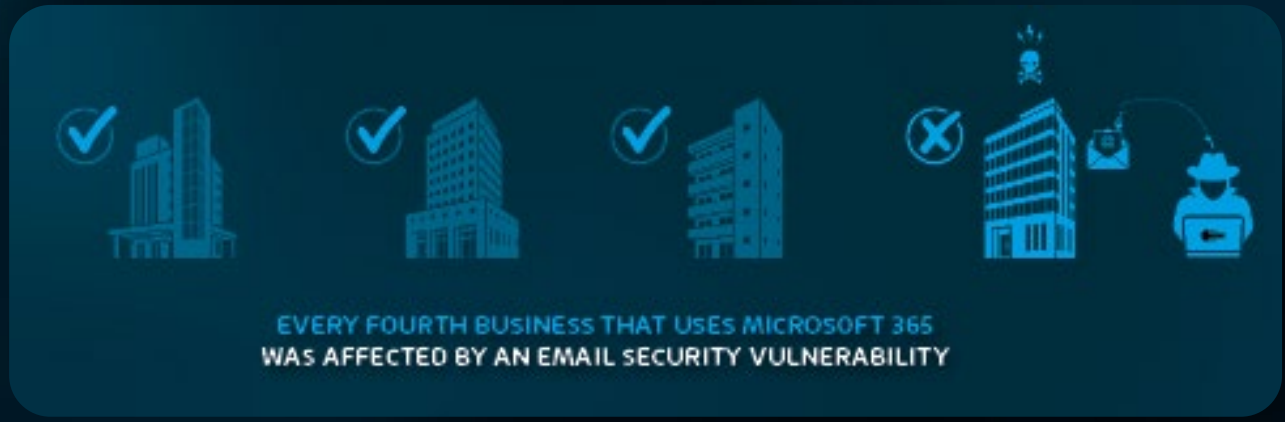
STEPHEN SIMONS

Head of Partner Management
Northern Europe

simons@hornetsecurity.com

CYBERTHREATS ON THE RISE

- 91% of all cyberattacks start with an email
- 1 in 5 businesses fall victim to ransomware, causing huge data and monetary losses
  - Ransomware demands range from US$100 to US$10,000,000
- 1 in 4 businesses using Microsoft 365 reported a security breach
  - Attackers gain access to sensitive data via malware or phishing emails and exploit it for their own benefit



HORNETSECURITY

HORNETSECURITY SECURITY LAB

- International team of developers and IT security specialists
- 24/7 monitoring of detection mechanisms
- Exclusive facts & figures (average):
  - 33120 new email-based threats observed on an average day
  - 12996 ransomware attacks per hour
  - 361 "sophisticated" phishing attacks per minute
  - 8 multi-vector (phone, email) fraud attacks per minute

HORNETSECURITY

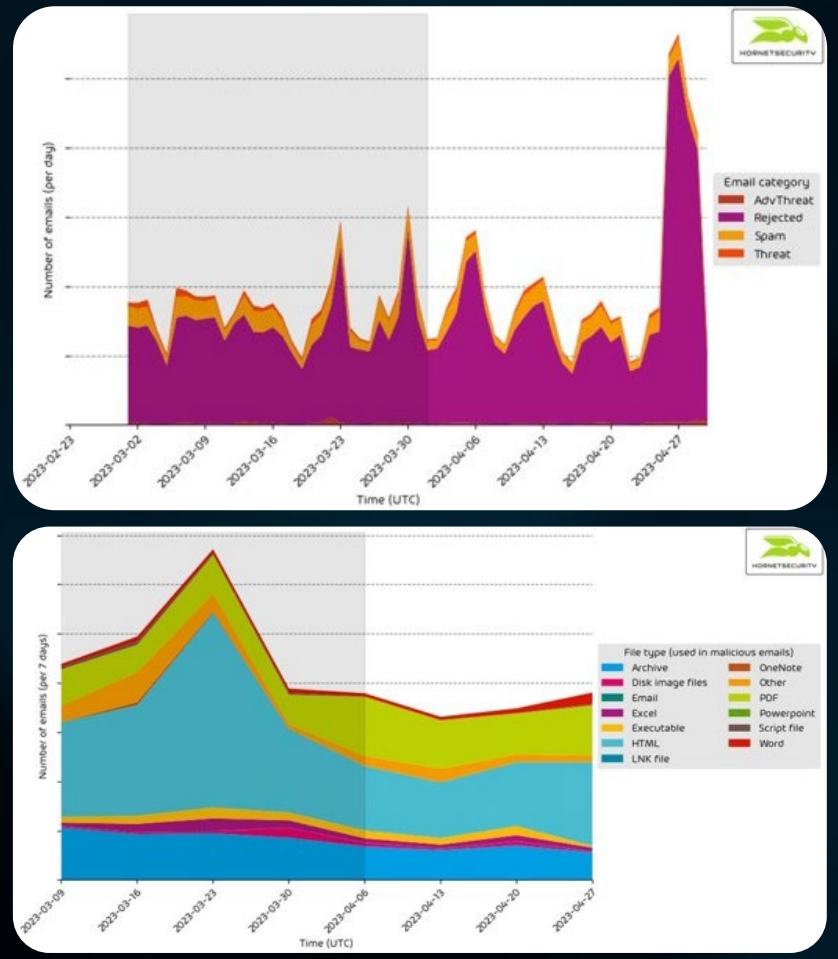


Fig. 1 & 2: Graphs of various email threats reported by the Hornetsecurity Security Lab

URM

GDPR Compliance

WEBINAR

Pauline Brace

Senior Consultant

Introduction

- Today's technology is not the villain
- Other people using technology for unfair or unlawful use of personal data for gain and profit are!
- Risk: A cyber-security event involving unauthorised disclosure is likely to represent a "failure to apply sufficient Technical and Organisation measures to protect personal data and the rights of individuals to expect their data to be processed securely. Article 32
- It also represents an "administrative" breach of the GDPR (Article 5)
- Lets take a look at those requirements.

GDPR Article 5

1. Personal data shall be:
    1. processed lawfully, fairly and in a transparent manner
    2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
    3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
    4. accurate and, where necessary, kept up to date;
    5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
    6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

GDPR Accountability Article 5(2)

- In the news: Head of UK bank resigns over privacy failure
- Common causes of compliance breaches relating to Article 5 and the principles:
  - Lack of internal information ownerhip
  - Unreliable evidence of decision making – burden of proof
  - Mandatory documentation and processes
    - No Record of Processing Activities (Article 30)
    - Unclear or non-existent privacy notices (Articles 13 and 14)
    - Insufficient User rights fulfilment
      - Right to be informed, access, secure processing, correction, objection, erasure, portability and legal remedy.
    - Poor third party supplier management, typically failure to perform due diligence/contractually binding guarantees (Article 28)
    - Privacy by design and by default (Article 25)
    - Data Protection Impact Assessments
    - Data Transfer Impact Assessments
      - Triggered by Change Management, project specifications, new systems or technologies, new suppliers

UK and EU Supervisory Authorities "Top" Penalties:

- **Failure to apply sufficient technical and organisational measures Article 32**
- Non-compliance with general data processing principles Article 5
  - Transparency – failure to fully inform data subjects (privacy notices Article 13/14)
  - Cookie policies) Article 5 and PECR
  - Unnecessary retention in identifiable form
- Insufficient legal basis for data processing (Article 6 and 9)
- Unlawful international data sharing (Article 44 – 50)
- Insufficient fulfilment of data subject's rights (Article 12 – 23)
- Poor management of third party suppliers (Article 28)
  - Due diligence
  - Contractually binding guarantees

Cyber Attack Motivation?
Why do other people want our data?

- Monetization – e.g. sale value, organized crime.
- Peer Group Kudos
- Revenge/damage
- Coersion/control
- Protesters/campaigners (publicity/social disruption/notoriety) – Hacktivism!
- Political gain
- Information warfare, espionage
- Media/Fame/Journalism
- Commercial advantage
- Identity theft

Unlawfully obtaining personal data without the data controller's permission is a criminal offence

GDPR Breaches – 2023 UK ICO Fines Summary

- Number and size of fines 8 – (Jan to July)
- Largest: Tik Tok £12.7m – Failure to apply DP Principles
- Estimated 1.4m children under 13 using Tik Tok
- 6 were fines for breaching The Privacy in Electronic Communications Regulations (PECR) consent rules
- total of over £1m
- UK's equivalent of the EU E-communications Regulations
- UK PECR fines are more frequent but tend to be lower in monetary value
- If a data protection complaint is upheld by the ICO, the data subject is entitled to pursue legal remedy in civil court – unlimited compensation depending on harm or distress (including non-material damages)
- Class Actions are permitted
- Cost of reputational damage

GDPR Breaches – 2022 UK Fines Summary

Organisation	Value	Reason
Interserve Group	£4.3m	Failure to provide sufficient organisational and technical security measures
Easylife Ltd	£1.2m	Insufficient lawful basis
Tavistock & Portman NHS	£78k	Failure to provide sufficient organisational and technical security measures
Clearview	£7.7m	Non compliance with general principles (also fined by other EU regulators for failing to co-operate with SA's)
Tuckers Solicitors	£98k	Non compliance with general principles

Plus 32 Reprimands and 23 Enforcement Notices issued in 2022

Largest ever GDPR fine – META at 1.2 billion Euros – Transferring data to US in breach of EUCJ ruling

Internal Misuse 2023 – 3 Prosecutions

- A former employee of the RAC has been prosecuted for obtaining the personal data of individuals involves in road traffic collisions after 21 drivers were harassed by claims companies.
- A former 111 call centre advisor has been found guilty and fined for illegally accessing the medical records of a child and his family.
- A former tracing agent pleaded guilty and was fined for illegally obtaining personal information to check if customers of a high street bank could repay their debts.
- Managing internal users of M365 and other systems is essential
- Training – trustworthiness and reliability
- Roles, responsibilities and competency
- Policies, processes and procedures
- Retention of personal data
- Rights, Rights, Rights

Scams

- Phishing and Vishing
- Romance Scams
- Emergency Scams
- Official Imposters
- Business Opportunities
- Courier Delivery Scams
- Home Repair Scams
- Tech Support Scams
- Advance Fee Scams
- Foreign Money Exchange Scams
- Bogus Debts
- Shopping Sprees
- Prizes

The Trans-Atlantic Data Privacy Framework

- a.k.a. Privacy Shield 2.0
- Adequacy decision by EU made July 23
- Facilitates EU to US personal data transfers
- But to “Certified entities” only
- Legal challenge inevitable
- Keep calm and carry on!

Information Security Standards

Demonstrating Assurance for Article 32 provision of technical and organisational security measures

- Cyber Essentials and Cyber Essentials +
- ISO 27001, ISO27002, ISO 27701
- NIST
- SOC
- SANS

Thank you!

365 TOTAL PROTECTION SUITE PLANS

NEXT-GEN SECURITY, BACKUP, COMPLIANCE & SECURITY AWARENESS FOR MICROSOFT 365

PLAN 1	PLAN 2	PLAN 3	PLAN 4
BUSINESS	ENTERPRISE	BACKUP	COMPLIANCE & AWARENESS
SPAM & MALWARE PROTECTION	ADVANCED THREAT PROTECTION	BACKUP & RECOVERY OF MAILBOXES & TEAMS	PERMISSION MANAGEMENT
EMAIL ENCRYPTION	EMAIL ARCHIVING	BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT	PERMISSION ALERTS
EMAIL SIGNATURES & DISCLAIMERS	EMAIL CONTINUITY	BACKUP & RECOVERY OF ENDPOINTS	PERMISSION AUDIT

PLAN 4
PHISHING & ATTACK SIMULATION
SECURITY AWARENESS
ESI® REPORTING

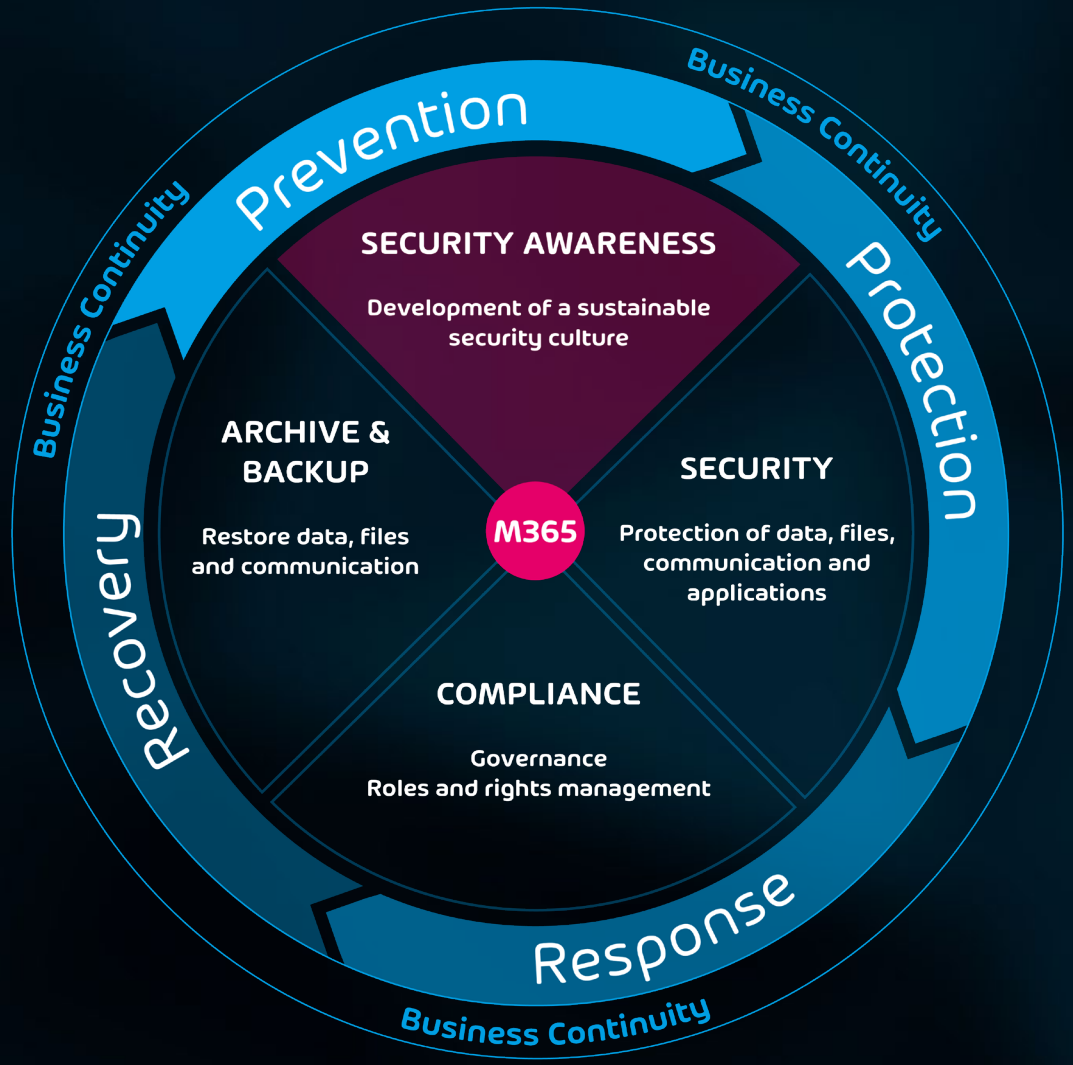
PLAN 4
COMMUNICATION PATTERN ANALYSIS
AI RECIPIENT VALIDATION
SENSITIVE DATA CHECK

HORNETSECURITY

NEXT-GEN SECURITY AWARENESS SERVICE

HORNETSECURITY

SECURITY AWARENESS SERVICE



ANY QUESTIONS?

HORNETSECURITY

THANK YOU!

HORNETSECURITY

HORNETSECURITY