M&S & Coop Cyber Incidents

2025

How were M&S Compromised?

Events

- **Initial Access**: Via social engineering the IT Service Desk reset the password for a privileged user
- **Server Access**: The user accesses the servers, probably by pivoting through Cloud. The attacker creates a new virtual machine and promotes it to a security database. All usernames and passwords are then extracted and exfiltrated, allowing passwords to be brute forced offline
- **Entra ID Access**: Scattered Spider target Identity Providers, including Entra ID. Accessing it through the Microsoft portal, creating new users and reset passwords for existing users.
- **Data Exfiltration**: With Domain Admin access, the attackers can access and exfiltrate data from any server. This is done through SaaS services, or through S3 buckets owned by the attackers
- **Encryption**: DragonForce ransomware is deployed, successfully evading security controls. The software is configured to encrypt all infected devices

What aspect of Cyber are you most worried about?

Have the M&S and Co-Op incidents increased the focus on cyber in your organisation?

FUNDAMENTALS

- Password management / Service Desk
- Anti-Virus
- Backups off site/immutable
- Secure enterprise firewalls
- Bit Locker Laptop Encryption
- Two Factor Authentication/MFA
- Wi-Fi secure – Main/Guest
- Cyber Insurance and where these are stored

EMAIL, WEB, & DEVICE SECURITY

- Email security – Mimecast
- Web Filter – Cisco Umbrella
- Microsoft Rings – enforced managed updates
- Enhanced monitoring software
- VPN for external users
- Cloud data lock downs (SharePoint)
- Mobile Management

TRAINING, EDUCATION, & CERTIFICATION

- Cyber Essentials Plus cert / NIST / ISO27001
- Penetration Testing
- Cyber policies kept up to date
- Mobile Management
- Phishing exercises
- User awareness training
- Retention policies
- ISQM1 Standard

PROACTIVE SECURITY

- T-Tech Managed Security & 24/7 Proactive Monitoring
- Manage, Detect, Respond
- Annual Reviews
- DMARC enablement
- Microsoft Secure Score

SECURITY MATURITY PILLARS

Themes

- Consider all the elements of the Security Pillars in detail
- Review Cyber Governance Code of Practice, NCSC exercise in a box and other NCSC guidance
- Have conversations with your suppliers (especially service/tech providers) about their cyber defences
- Risks around social engineering, securing social media accounts and not over-sharing on public profiles
- Plan and training for everyone - little and often is the best approach
- Don't make it someone else's problem

What is your key takeaway / action from today?

Questions?

Ian Pay - Ian.Pay@icaew.com
Daniel Teacher - Daniel.Teacher@ttech.uk.com
Radhika Modha -