MALTA INFORMATION TECHNOLOGY AGENCY

Cyber Threats & Government Aid

The SME Conference – SME Year in review - 2019

31th October, 2019

CYBER SECURITY MALTA

Digital Security Your Priority

mita

Definition of Cyber Security Incident

- **(NIS) Security of network and information systems** means the ability of network and information systems to resist…any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted…

- **(NIS) Incident** means any event having an actual adverse effect on the security of network and information systems

- **(NIST) Cybersecurity Incident** – A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.

Taxonomy of a Cyber-Attack

- Passive cyber-attack
  - **attempts to gain access or make use of information from the system without interaction**
  - Reconnaissance, surveillance, wiretapping, port scanning, keystroke logging, data scraping, backdoor, eavesdropping, vulnerabilities, war driving, dumpster driving

- Active cyber-attack
  - **attempts to alter a system or affect an operation**
  - Denial-of-service attacks, email spoofing, phishing, man-in-the-middle, ping of death, overflows, direct access access, social engineering, tampering, privilege escalation, viruses, worms, malicious code, zero-day exploit

Impact of a Cyber-Attack

University of Kent – "*At least 57 negative impacts from cyber-attacks*" (2018)

- Physical / digital
  - Damaged or unavailable, theft, compromised, infected, exposed or leaked, corrupted, reduced performance, bodily injury, pain, loss of life, prosecution, abuse, mistreatment, identity theft
- Economic
  - Disrupted operations, disrupted sales, reduced customers, reduced growth, reduced investment, fall in stock price, theft of finances, loss of finances or capital, regulatory fines, investigation costs, PR response costs, compensation payments, extortion payments, loss of jobs, scammed.

Impact of a Cyber-Attack - continued

- Psychological
  - Confusion, discomfort, frustration, worry & anxiety, feeling upset, depression, embarrassed, shameful, guilty, loss of self-confidence, low satisfaction, negative changes in perception
- Reputational
  - Damaged public perception, reduced corporate goodwill, damaged customer relationships, damaged supplier relationships reduced business opportunities, inability to recruit desired staff, media scrutiny, loss of key staff, loss or suspension of accreditation, reduced credit score
- Social / Societal
  - Negative changes in public perception, disruption in daily activities, negative impact on nation, drop in internal organizational staff

Cyber Security – European facts

- The average cost of a cybersecurity breach increased 6.4% in 2018
- 165m Europeans lacked basic digital skills in 2017
- 4000 ransomware attacks per day
- 95% of cyber incidents were enabled by some type of human error
- EU-wide - Europol EC3, ENISA, NIS Directive, EU Certification Framework, EU Cyber Security Act, Blueprint for rapid emergency response, Securing the electoral process, The European Cybersecurity Industrial, Technology and Research Competence Centre, Cyber Defence, GDPR, other sectorial cybersecurity obligations

Top 15 threats to Cyber Security – ENISA's Threat Landscape Report 2018

Malware, Web Based Attacks, Web Application Attacks, Phishing, Denial of Service, SPAM, Botnets, Data breaches, Insider threat, Physical manipulation / damage / theft / loss, Information leakage, Identity Theft, Cryptojacking, Ransomware, Cyber espionage

What? Where? How? Who?

Number 15 – Cyber Espionage

- Primary motivation is intelligence gathering

- Usually a complex targeted attack using multiple technologies of malware, repurposed ransomware and phishing, living-of—the-land

- Motivated by financial, political, or ideological gains

- Infiltration of third- and fourth-party supply chain partners (including software suppliers) with weak cybersecurity programs

- Primary targets are the industrial sector, critical and strategic infrastructures, government entities, transportation, telecommunication providers, energy companies, hospitals, banks, business leaders

Number 15 – Cyber Espionage - continued

- Recently observed threats
  - Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies (Jun 2018)
  - Phishing attack allegedly targeted the Democratic National Committee (DNC) just a few days after the 2018 midterms (Jan 2018)

- Mitigation measures
  - Hire talented individuals, risk assessment, identify mission critical roles, information security policy, conduct regular vulnerability assessments, implement need-to-know principles, implement content filtering solutions, physical security, user education & awareness, logging & monitoring tools

Number 14 – Ransomware

- Attackers gain ownership of files or devices and blocks the real owner from accessing them, demanding a ransom in cryptocurrency to return ownership
- Vulnerabilities via outdated software, phishing emails, malicious files
- A shift towards towards cryptojacking rather than ransomware attacks was observed
- In the first half of 2018, cryptocurrency mining detections increased by 96% from the previous year

Number 14 – Ransomware - continued

- Mobile malware is up 33%
- 81% of total infections were organisations
- 85% of malware attacks on healthcare were ransomware
- 44% more users encountered miners in Q1 2018
- 39% of the global malware data breaches caused by ransomware
- 93% of phishing emails were related to ransomware
- 65% of the ransomware attacks were delivered via email and 35% via malicious URLs
- 66% of companies agree that ransomware is a serious danger but less than 13% were prepared for it

Number 14 – Ransomware - continued

- Recently observed threats - WannaCry
  - Estimated total global damages of $4 billion worldwide
  - Infected more than 200,000 computers across 150 countries
  - NHS, Deutsche Bank, FedEx, Hitachi, Honda, Renault, Nissan UK, O2
  - Based on a combination of technically simple exploits
  - Replicates without human interference
  - NHS 19,000 cancelled appointments & £92m in damages and upgrades
  - More than 312 ransom payments were made

- Mitigation measures
  - Risk assessment, identify mission critical roles, information security policy, need-to-know principles, account management procedure, content filtering solutions, user education & awareness, network segmentation, data encryption, access control, logging & monitoring tools, end-point protection software, backups, vulnerability and patch management system

Number 13 – Cryptojacking

- Applications that use a victim's processing power to mine cryptocurrencies without the victim's consent
- Cryptomining can be browser-based such as JavaScript and WebAssembly, cloud spaces or Operating Systems, POS terminals, vending machines…
- The Cybercrime-as-a-Service earn real world money including insider mining
- New cryptocurrencies provide higher levels of transaction anonymity such as Monero or Ethereum

Number 13 – Cryptojacking - continued

- The Economics of Cryptojacking
  - During the first half of 2018, cryptominers have generated $2.5 billion for their users
  - An adversary controlling 2,000 devices with Monero miners generates $500 a day
  - Cryptojacking malware grows 629% in Q1 of 2018

- Mitigation measures
  - Risk assessment, identify mission critical roles, information security policy, conduct regular vulnerability assessments, implement content filtering solutions, user education & awareness, account management procedure, content filtering solutions, access control, loggin & monitoring tools, end-point protection software, backups, vulnerability and patch management system

Number 12 – Identity Theft

- Digging through trash or mailboxes looking for bank statements, copies of tax returns and other documents that have personal information
- Legitimate software used in campaigns like Chrome extensions, mobile apps, websites, Facebooks
- Legal and civil, bank accounts, home addresses, accounting records, health, contacts
- The fraud committed from the theft of PI information
- Telephone impersonation, network administrators
- 30% increase in phishing links on social media

Number 12 – Identity Theft - continued

- Recently observed threats
  - W2 scam is an attack that spoofs an executive member of finance or HR department for employees' records
  - New account fraud – Loans, credit cards, access to restricted areas

- Mitigations measures
  - Risk assessment, identify mission critical roles, information security policy, implement need-to-know principles, implement content filtering solutions, physical security, user education & awareness, data encryption, access control, logging & monitoring tools, background checks, MFA, SSO, strong cloud security, strong encryption methods for sensitive data, secure connections (open WiFi), user account management, logging and monitoring.

Number 11 – Information Leak

- Usually caused by an internal individual’s action, a process failure, technical error or misconfiguration
- Privacy policies, terms & conditions drive users to voluntarily waive ownership / custody of their data
- 72% of incidents were unintended disclosure, followed by 27% from hacking or malware
- 50% of unintended disclosure are due to lost devices
- Primary threat comes from insiders

Number 11 – Information Leak - Continued

- Average cost of data disclosure is $3,86M, +6.4%
- 29% of all incidents originate from internal actors, not necessarily intentional, 22% are system administrators
- Mitigations measures
  - Risk assessment, information security policy, conduct regular vulnerability assessments, implement need-to-know principles, content filtering solutions, physical security, user education & awareness, account management procedure, data encryption, access control, logging & monitoring tools, end-point protection software, vulnerability and patch management system, MFA, SSO, strong encryption methods for sensitive data, anonymise & secure data according to GDPR or other regulations, data access and classification policies

Number 10 - Physical manipulation, damage, theft or loss

- Physical access to a device gives opportunities to attackers ex. ATM fraud and POS attacks
- Most common theft locations are employee’s private vehicles, airports and hotels
- 33% of organisations lack a physical security policy
- 25% of data breaches in the financial sector are due to the loss or theft of devices
- Mitigation measures and techniques
  - Risk assessment, information security policy, implement need-to-know principles, physical security, user education & awareness, account management procedure, device encryption, end-point protection software, MFA, SSO, data access and classification policies, physical inventory, physical security for sensitive areas, information security policy, backups

Number 9 – Insider Threat

- Three types of insider threats; Malicious, negligent, compromised
- 77% of data breaches are from insiders
- 47% of medium-sized companies rated the insider threat as their primary security concern
- 53% of the companies had at least one incident of insider threat in the last 12 months
- 20% of them had more than six incidents in the same period
- Phishing is the biggest weakness

Number 9 – Insider Threat - continued

- Most dangerous insider threats are employees, IT admins, contractors, temporary workers, business executives, customers
- Most attractive data sets are confidential business information, privileged account information, sensitive personal information, IP, employee data, infrastructure data
- Mitigation measures
  - Risk assessment, identify mission critical roles, information security policy, implement need-to-know principles, user education & awareness, logging & monitoring tools, account management procedure, data encryption, MFA, SSO, strong encryption methods for sensitive data, anonymise & secure data according to GDPR or other regulations, data access and classification policies

Number 8 – Data Breach

- Does not specifically apply as a threat but reflects a successful malicious attempt
- Cloud infrastructure is the most attractive vector
- 27% of all data breaches are health related
- 99% of data is not encrypted
- 56% of breaches are identity theft related
- 36% decrease in the number of incidents
- 28% increase in the number of records breached

Number 8 – Data Breach - continued

- Notable events
  - Huazhu Hotels Group 22.3 GB of data, 130 million customers' personal data and booking information
    - Cause: Accidentally uploaded to the internet
  - Facebook: A weakness in the "Search" capability of the platform exposed ca. 2B user information publicly
    - Cause: Software vulnerability
  - Company affiliated with FedEx exposes data
    - Cause: Software misconfiguration on the cloud
- Mitigations measures
  - Risk assessment, information security policy, conduct regular vulnerability assessments, implement need-to-know principles, content filtering solutions, physical security, user education & awareness, account management procedure, data encryption, logging & monitoring tools, end-point protection software, vulnerability and patch management system, access control, MFA, SSO, strong encryption methods for sensitive data, anonymise & secure data according to GDPR or other regulations, data access and classification policies, data classification, least privilege / need to know

Number 7 - BOTNETS

- A group of orchestrated (usually hijacked) physical devices by exploiting known vulnerabilities such as IoTs
- Scalable, autonomous, swarm attack, sharing of collected intelligence, silent army, can be updated
- Serve multiple malicious activities
- 97% delivery of of spam, social media ads, IoTs, banking malware
- Takes just one day to exploit a new vulnerability

- Mitigations measures
  - Risk assessment, information security policy, conduct regular vulnerability assessments, data encryption, access control, logging & monitoring tools, end-point protection software, vulnerability and patch management system, network firewalls, traffic filtering, content filtering, IP address black-lists

Number 6 - SPAM

- The abusive use of messaging technologies to flood users with unsolicited messages
- The average daily spam volume is 295,62 billion
- Low cost means of sending messages
- Resource consuming and costly for recipients
- Consistent decrease since 2008
- Abuse of online forms
- Mitigations include
    - Risk assessment, information security policy, conduct regular vulnerability assessments, implement need-to-know principles, content filtering solutions, user education & awareness, account management procedure, logging & monitoring tools, end-point protection software, access control, least privilege / need to know, email security policy, disable automatic execution of code

Number 5 – Denial of Service

- Makes a device or network resource unavailable to its intended users by disrupting its services
- Cause nationwide failures for businesses and critical systems
- DDoS for hire as-a-service is rising by 16%
- Mitigations include
  - DoS managed services, firewalls, web application firewalls, IPS/IDS systems, network flow, Access Control Lists and Intelligent DoS mitigation tools, identify critical devices
  - Internet Service Providers, carries and cloud providers play a key role in mitigating DoS attempts

Number 4 - Phishing

- Crafting of messages that use social engineering to lure victims via SMS, mobile messaging, traditional messaging, social media
- 90% of malware infections and 72% of data breaches in organisations originate from phishing attacks
- 71% of APT groups have used spear-phishing as infection vector
- The preferred way of compromising an organisation
- Malicious attachments or URLs

Number 4 – Phishing - continued

- Organised criminal groups target rich individuals, people with access to financial accounts or sensitive business data
- Malicious actors are focusing on enterprise targets – a shift from the previous years
- Phishing attacks on mobile devices have grown by an average of 85% since 2011
- Mitigations include
  - Risk assessment, information security policy, content filtering solutions, user education & awareness, account management procedure, logging & monitoring tools, end-point protection software, vulnerability and patch management system, access control, data access and classification policies, least privilege / need to know, email security policy, disable automatic execution of code, least privilege account on devices, educate users and raise awareness

Number 3 – Web Application Attacks

- A direct or indirect attempt to exploit a vulnerability or a weakness in the services and applications on the web
- Businesses are investing more on web applications detection, protection and defence
- More businesses are becoming dependent on web services
- Legacy web app exploits are still among the top 20
- SQL injection continues to lead the attacks types (51%)
- Local file inclusion (34%)
- Mitigations include:
  - Risk assessment, information security policy, account management procedure, logging & monitoring tools, vulnerability and patch management system, access control, data access and classification policies, least privilege / need to know, segregation, implement authentication and authorization mechanisms, WAF, traffic filtering, perform input verification

Number 2 – Web Based Attacks

- Use web systems and services as the main surface for compromising a victim

- Browser exploitations and injections (including extensions), websites, Content Management System (CMS), web services, redirection and man-in-the-browser attacks, spamming campaign, bank trojans

- Malware and exploitation techniques rely heavily on these attacks as the delivery mechanism

Number 2 – Web Based Attacks - continued

- Internet Explorer (CVE-2018-8174) and Flash (CVE-2018-4878) have been the most weaponised vulnerabilities
- Drive-by downloads – cybercriminals look for insecure websites and plant malicious scripts into HTTP or PHP code
- Mitigations include:
  - Web traffic filtering, web traffic filtering, web-servers and web-browser updates, vulnerability assessment, risk assessment, avoid third-party plugins, end-point protection,

Number 1 - Malware

- Accounts for 30% of all data breaches
- WannaCry and Petya
- Blurred lines between cyber criminals and cyber espionage actors
- Encrypted command & control communication has increased by 300%
- Abuse of legitimate encrypted channels is growing
- Use of blockchain technology is expected to be leveraged
- Malware authors increasingly targeting IoT devices

Number 1 – Malware - continued

- Malware is polymorphic
- 79% of the detected malware in organisations were targeting Windows
- Endpoints are usually targeted blurring organisation perimeter and mobility
- Mitigations include:
  - Risk assessment, information security policy, content filtering solutions, user education & awareness, account management procedure, logging & monitoring tools, end-point protection software, vulnerability and patch management system, access control, data access and classification policies, least privilege / need to know, email security policy, disable automatic execution of code, least privilege account on devices, malware detection, network protection threat hunting, MISP, triangulation

SECURE

TOWARDS A SECURE CYBER SPACE FOR BUSINESS

B SECURE

- Fully subsidized by the Maltese Government
- First come, first served through the a review board
- Variety of courses covering
  - Introductory for executives and professionals
  - CISA, CISM, Web Application Protection, CCSK, CISSP
- Vulnerability Assessments
  - Executed remotely and directly with Acronis International GmbH
  - Up to 10 external IPs for SMEs
  - Up to 20 external IPs for large organizations
- Penetration Testing
  - Large organizations must provide Acronis International GmbH remote and onsite access to systems
  - SMEs must provide Acronis International GmbH remote access to systems only

mita

MALTA INFORMATION TECHNOLOGY AGENCY

Thank You

/MITAofficial @MITAmalta info.mita@gov.mt