PROFiT
Prevention of Fraud in Travel

THE COUNTER FRAUD CAMPAIGN 2019

PART 20: DEFENSIVE SOFTWARE

Prevention of Fraud in Travel (PROFiT) and the Fraud Intelligence Network (FIN) are working with the City of London Police to reduce fraud in the travel industry. PART 20 is a brief overview of defending your organisation against cybercrime.

PROFiT is the only official travel industry counter fraud body. We work on your behalf to carry out analysis and research, disseminate best practice and disrupt crime.

Find out how you can join the fight against crime. Contact via: contactus@profit.uk.com

BACKGROUND

1.0 Over the past few weeks we have identified that the internet can be a hostile environment for organisations to operate in. There are a range of hostile actors and threats which can disrupt your business. This week we will look at the software suite that every organisation should have in place and some useful protocols that protect your business and its staff.

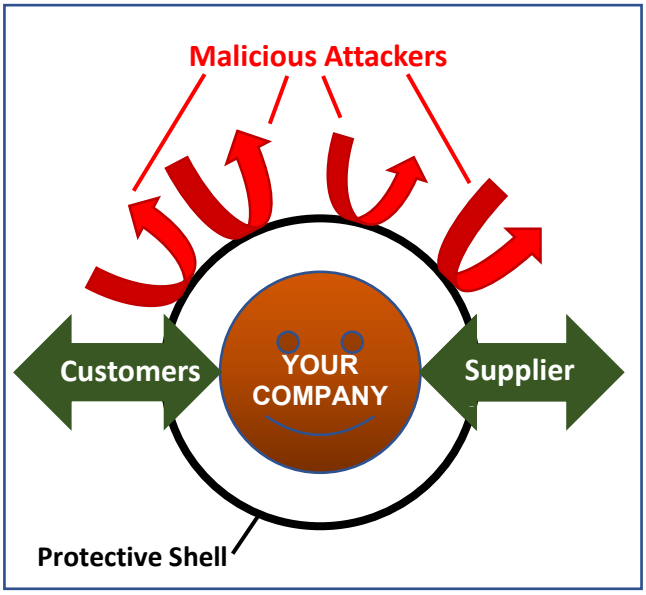
PERFECTING YOUR DEFENCE – THE BASIC STRUCTURE

2.0 In order to perfect your systems defences you are aiming to throw a protective shell around your organisation, which denies access to malicious actors whilst permitting seamless traffic to flow between you, your customers, and suppliers. This is what the police refer to as '**target hardening**' and it is the responsibility of every organisation and individual to take steps to secure themselves.

2.1 You are aiming to make it as hard as possible, without affecting your business, for malicious actors to exploit weaknesses in your systems to gain access and commit crime. Despite what commercial products may imply, there is no single solution that will effectively defend against all the threats that are out there. It is imperative therefore that defensive solutions are layered in a way that they complement each other and cover your business against most threats.

2.2 Applying this concept to your business you will need to have in place:

- **A Firewall,**
- **Anti-Virus software,**
- **Anti-Malware software,**
- **Anti-Spyware software,**
- **Systematic Backup, and**
- **A Password System.**



FIREWALLS

2.3 A firewall is software that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. The purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely. In effect a firewall acts like the front door to your house.

2.4 All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet your specified security criteria. You need a firewall to protect your confidential information from those not authorised to access it and to protect against malicious users and accidents that originate outside of your network. One of the most important elements of a firewall is its access control features which distinguish between good and bad traffic.

2.5 Even with a firewall, there are still many areas of risk for your network. The most obvious is malware. Another well-known threat, not covered by your firewall, is spam. As we have seen in previous weeks spam often contains viruses and phishing emails; it is also a direct security threat. SEE Email Campaign issue 17 Spam and Malware).

2.6 Unfortunately a firewall is no longer enough to protect a company network. Other security solutions to combat the threats outlined above are also necessary, as well as proper staff training. One of the best ways to protect against the main threats not covered by a firewall is to use a Unified Threat Management (UTM) device. UTM devices are multi-purpose security solutions which have a minimum of a firewall, Virtual Personal Network (VPN), anti-virus and intrusion detection/prevention. Some UTMs (sometimes known as super UTMs) also incorporate capabilities such as web filtering (blocking problematic web sites), Spam blocking and spyware protection.

ANTI-VIRUS SOFTWARE

2.7 Antivirus software is designed to prevent, search for, detect, and remove known software viruses, and other malicious software like worms, trojans, adware, and more. These tools are critical for users to have installed and kept up to date because a computer without antivirus software protection will be infected within minutes of connecting to the internet.

2.8 The bombardment against your computer systems is continual, which means antivirus companies must update their detection tools regularly to deal with the more than an estimated 60,000 new pieces of malware created daily. Updates are usually rolled out through a web-based upgrade sent out when new threats are identified. You should always make sure your antivirus software is set to automatically update so that you retain the fullest protection.

2.9 Antivirus software was originally designed to detect and remove viruses from computers, but it can also protect against a wide variety of threats, including other types of malicious software, such as keyloggers, trojans, worms, rootkits, spyware, adware, botnets and ransomware. Not every type of cyberattack can be prevented by anti-virus software, but it can be an asset when trying to prevent intrusion into a computer.

ANTI-MALWARE SOFTWARE

2.10 Antivirus software usually deals with the older, more established threats, such as trojans, viruses, and worms. Anti-malware, by contrast, typically focuses on newer threats, such as polymorphic malware and malware delivered by zero-day exploits. A zero-day exploit is a cyber-attack that occurs on the same day that a weakness is discovered in software. At that point, it is exploited before a fix becomes available from the software creator.

2.11 Think of it like this: anti-malware protects against brand new threats whilst anti-virus protects users from lingering, predictable-yet-still-dangerous malware. Some types of antivirus software and some UTM devices combine the antivirus and antimalware software functions so that they undertake both tasks.

ANTI-SPYWARE SOFTWARE

2.12 Spyware commonly comes in one of four different forms;

- **Adware** is unwanted software designed to place advertisements on your screen. Adware generates revenue for its developer by automatically displaying online advertisements in the user interface of the software or on a screen that pops up in the user's face during the installation process. Adware can hide malware.

- **System Monitors** can enter your systems, hide, and capture everything you do on your computer recording all keystrokes, emails, chat-rooms dialogue, websites visited and programs that are used.
- **Tracking Cookies**. Cookies are text files and so cannot be used to spread viruses and they cannot access your hard drive. However, tracking cookies can identify all information that you share through your computer such as passwords, personal and financial information. A tracking cookie can be a threat to privacy and financial information.
- **Trojans**. As we have previously seen a trojan is a program that looks legitimate but is in fact used by malicious actors for cybercrime and hacking.

2.13 Anti-spyware software is a type of program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed. Detection may be either rules-based or based on downloaded definition files that identify currently active spyware programs. Whilst some threats can be dealt with by both anti-virus an anti-spyware software only anti-spyware software can prevent criminals controlling your computers microphone and camera to spy on you which anti-virus is generally not able to deal with.

SYSTEMATIC BACK-UPS

2.14 A system back-up is the process of backing up the operating system, files, and system specific useful and essential data. During a back up the software takes a snapshot of the state, files and data of a computer system and duplicates that data elsewhere to form a safely stored duplicate that can be used to reinstall them in the event that the primary system is corrupted, deleted or lost.

2.15 There are four common types of data back up:

- **Full back-up**.
  A full backup is when every single file and folder in the system is backed up. A full backup takes longer and requires more space than other types of backups but the process of restoring lost data from backup is much faster.
- **Incremental back-up**.
  With incremental backup, only the initial backup is a full one. Subsequent backups only stores changes that have been made since the previous backup. The process of restoring lost data from backup is longer but the backup process is much quicker.
- **Differential back-up**.
  Differential backup is similar to an incremental backup. With both, the initial backup is a full back up and subsequent backups are only on changes made to files since the last backup. This type of backup requires more storage space than incremental backup does, but it also allows for a faster restore time.
- **Mirror back-up**.
  A mirror backup, as the name implies, is when an exact copy is made of the source data. The advantage of mirror backup as opposed to full, incremental, or differential backups, is that you're not storing old, obsolete files. When obsolete files are deleted, they disappear from the mirror backup as well when the system backs up. The downside to mirror backup is that if files are accidentally deleted, they can be lost from the backup as well if the deletion isn't discovered before the next scheduled backup.

2.16 There are different costs involved in each of these back-up choices and you need to work out the most suitable method for your business. We would recommend that you not only use one of the common backup types, but also back up twice - physically and online. This gives you onsite and offsite backups and makes the system more resilient to give more scope to restore your files if they become locked or corrupted through a malicious act.

A PASSWORD SYSTEM

2.17 The previous edition of the email campaign covered passwords in some depth and gave the latest official advice on how to create memorable but strong passwords. These passwords should be managed carefully. For example, passwords should be changed, periodically but not too regularly, so that it is harder for them to be compromised. Some software houses also offer 'password managers' which generate password solutions for users, but this can result in users being offered

gobbledygook in the form of a string of meaningless and difficult to remember letters, numbers and symbols.

E-MAIL SECURITY PROTOCOLS & QUAD9

3.0 There are several email protocols which you should adhere to in order to maintain your systems security. These protocols exist because the basic email protocol used to send emails, called Simple Mail Transfer Protocol (SMTP) does not include authentication processes. The email policies that you should adopt to remedy this omission include:

- **Sender Policy Format** (SPF)
  When you send an email it contains certain coding, which is hidden from view, in the header. One piece of coding tells the receiving server the address to return information when there is a problem – so it is the code which bounces back to tell you that there was a problem with delivery of your message. This code is known as the 'return path'. SPF looks at the 'return path' value to validate the originating server.

  SPF therefore improves the chances of your email arriving at the intended recipient over an email that does not have SPF. But as the 'return path' can be spoofed the recipient can still receive an email sent from a malicious actor because it is the recipient's ISP that verifies the 'return path'.

- **DomainKeys Identified Mail** (DKIM)
  Spoofing emails from trusted domains is a popular technique for malicious spam and phishing attacks; DKIM is an email security standard designed to make sure that messages were not altered during transit makes it harder to spoof emails from domains that use it. DKIM uses public-key cryptography to sign each email with a private key as it leaves the sending server.

  The recipient servers can then use a public key published to a domain's DNS to verify the source of the message, and check that the body of the message has not changed during transit. Once the check made using the private key is confirmed using the public key by the recipient's server, the message passes DKIM and is considered authentic. An additional benefit of DKIM is that Internet Service Providers (ISPs) use it to build a reputation for your domain. As you reduce spam and bounces then over time you develop a good email reputation with ISPs which improves delivery.

- **Domain based Message Authentication, Reporting and Confirmation** (DMARC)
  DMARC is a protocol that uses SPF and DKIM to determine the authenticity of an email message. DMARC requires both SPF and DKIM to fail for it to act on a message. The way it works is to help email receivers determine if the purported message "aligns" with what the receiver knows about the sender. If not, DMARC includes guidance on how to handle the "non-aligned" messages. A DMARC rejection causes email receivers not to deliver emails failing the DMARC checks.

  Where a group of users adopt DMARC they in effect have 'herd immunity' as it is not possible for a malicious actor to intercede by spoofing any of their emails so preserving the integrity of the group's communications. Adopting DMARC amongst a group prevents criminals spoofing one member's emails to other members saying that the bank account has been changed and thus diverting funds. It also prevents criminals creating a realistic invoice and spoofing one group members' email account to seek fraudulent payment from the others.

  You can obtain the benefit of free and effective DMARC from the Global Cyber Alliance at: https://dmarc.globalcyberalliance.org

- **Quad9**
  Just like your home every device connected to the internet has an address known as an Internet Protocol (IP) address. Domain Name System (DNS) is a protocol for exchanging data on the internet using the IP address system. An email address is matched to a domain name and this needs to be matched to an IP address in order to send the data. The mail server uses DNS to match the address you wish to send the message to, to its destination and deliver

the email. The public key needed to decode your DKIM signature can be accessed from the DNS. This is needed to verify your identity as the sender.

Quad9 blocks against known malicious domains, preventing your computers and IoT devices from connecting to malware or phishing sites. Whenever a Quad9 user clicks on a website link or types in an address into a web browser, Quad9 checks the site against a list of domains combined from multiple threat intelligence partners. Each threat intelligence partner supplies a list of malicious domains based on their heuristics which examine such factors as scanned malware discovery, network IDS past behaviour, visual object recognition, optical character recognition (OCR), structure and linkages to other sites, and individual reports of suspicious or malicious behaviour. Based on the results, Quad9 resolves or denies the lookup attempt, preventing connections to malicious sites when there is a match.

By filtering out IP addresses that have been proven to have been used maliciously Quad9 effectively prevents infected spam and communications from nefarious sources and prevents your members connecting to the same bad places.

You can obtain the benefit of free and effective QUAD9 from the Global Cyber Alliance at: https://www.globalcyberalliance.org/quad9/

OTHER SECURITY PROTOCOLS

4.0 There are numerous other protocols that relate to IT security. Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data sent over an Internet Protocol network. It is used in virtual private networks (VPNs). Perhaps the most significant protocol for non-IT staff is the HTTPS protocol which can be identified by the green padlock symbol in the address bar.

4.1 Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network and is widely used on the Internet. The principal motivations for HTTPS are authentication of the accessed website, protection of the privacy and integrity of the exchanged data while in transit. It protects against man-in-the-middle attacks. The bidirectional encryption of communications between a client and server protects against eavesdropping and tampering of the communication.

4.2 A user should only trust an HTTPS connection to a website if all of the following are true:

- The user trusts that the browser software correctly implements HTTPS with correctly pre-installed certificate authorities.
- The user trusts the certificate authority to vouch only for legitimate websites.
- The website provides a valid certificate, which means it was signed by a trusted authority.
- The certificate correctly identifies the website (e.g., when the browser visits "https://example.com", the received certificate is properly for "example.com" and not some other entity).
- The user trusts that the protocol's encryption layer (SSL/TLS) is sufficiently secure against eavesdroppers.

MISSED A PREVIOUS EDITION?

If you have missed a previous edition of the email campaign let us know and we can send you FREE a copy: contactus@profit.uk.com

Like what we do to protect you?

We are always short of funds and need your support.

Find out how you can join PROFiT and fight fraud by emailing contactus@profit.uk.com

Next Week: Part 21 The end of the 2019 campaign