Image: Peter Kasprzyk / Unsplash.com

Prof Kevin Curran Professor of Cyber Security
kj.curran@ulster.ac.uk
Ulster University, Derry

Reflections on the NCSC cyber threat to UK business 2017-2018 report

Professor Kevin Curran, Professor of Cyber Security at Ulster University, here summarises the cyber risk trends - both of the present and of the future - that the National Cyber Security Centre ('NCSC') identifies in its 'The cyber threat to UK business 2017-18 report" ('Threat Report'), and the actions the NCSC advises that businesses take in order to mitigate those risks.

Cyber crime damage is now measured in the trillions annually and is fast becoming the leading criminal damages threat to organisations. The internet has become the core of modern life and e-commerce the life blood of many organisations. Today more than half of attacks involve organised criminal groups. Finance and espionage are the top two motives combining to account for 93% of breaches. The Threat Report examines how cyber activities over the past 12 months have impacted the reputation of businesses and their bottom line.

Cyber trends

The main incidents in 2017 included ransomware and distributed denial of service attacks, massive data breaches, supply chain compromises and fake news and information operations.

Ransomware

Ransomware is simply a modern IT horror. Once a device is infected, it typically encrypts all potentially important documents on the computer and any attached network drives, and starts a counter that, once it reaches zero, removes the files. The only solution to most of these is to pay the scammers. It is the deadliest scam at this moment and will increase due in part to the rise of cryptocurrencies, which allow the scammers to remain anonymous. Recently, we have also seen a dramatic rise in ransomware distributed denial of service ('DDoS') attacks using cryptocurrencies as the payment method. Here the hackers threaten to bring a site to its knees unless a ransom is paid.

The NCSC's mitigations against ransomware and DDoS attacks include the deployment of critical security patches as soon as possible, using always-on antivirus solutions to scan new files, conducting regular vulnerability scans alongside actioning critical results, implementing application whitelisting technologies to prevent malware running on hosts, implementing a policy of least privilege for all devices and services and establishing configuration control and management.

Data breaches

The number and scale of data breaches increased in 2017, with Yahoo finally admitting that all of its 3 billion customers had been affected by the 2013 breach. The techniques used in many cases were not that advanced but rather relied on exploiting unpatched vulnerabilities and spear phishing emails. It can be argued that a major factor concerning so many data breaches last year is simply an indication of where we are in time, as we are situated between a time where companies really face no penalties for poor storage and protection of data (apart from reputation loss) and a future world where organisations will be fined enormous sums for allowing data to leak. People are also in a semi-state of ignorance (or deliberate ignorance) of safe computing practices. The Threat Report gives examples of data breaches including Equifax (145 million accounts) and Verizon (14 million accounts).
The NCSC's mitigations against data breaches include using up-to-date and supported operating systems and software, deploying critical security patches as soon as possible, implementing application whitelisting technologies to prevent malware running on hosts, using firewalls and network segregation to protect services, deploying an always-on antivirus solution that scans new files, performing regular vulnerability assessments against both internal and external services to scan for any insecure configuration, implementing a policy of 'least privilege' for all devices and services, using multi-factor authentication to protect sensitive information, ensuring that all services are protected by strict authentication and authorisation controls, using password managers to help prevent password reuse between systems and implementing a practical monitoring and alerting service.

Supply chain compromises

2017 saw some significant examples of supply chain attacks which included the compromise of a large number of managed service providers ('MSPs'), enabling access to commercially sensitive data from them and their clients. This is another case of hackers seemingly endlessly finding new vectors of attack as operating system giants and software companies take steps to patch known exploits. This new mode of compromise is through the distribution of software libraries and programs containing exploits which trick unsuspecting users into installing. Just last year, the official repository for the widely used Python

1. Available at https://www.ncsc.gov.uk/cyberthreat

continued

programming language was infected with modified code packages which were uploaded to the Python Package Index. The packages contained the same code as the upstream libraries, but the hackers had also added an installation script which was modified to include malicious code. This was a dangerous precedent. MeDoc and CCleaner are two more examples that were compromised at source, resulting in their customers being infected with malware when downloading the software/updates. The NCSC's mitigations against supply chain attacks are to work with companies certified through the NCSC Cyber Essentials Scheme and follow the principle of 'least privilege,' especially for external parties that may need remote access into networks for specific administrative tasks.

Fake news and information operations

Social media provides nefarious actors with opportunities to cause reputational damage to a business. The majority of the publicity in fake news went to political examples but businesses have also suffered. The Threat Report does acknowledge that fake news is not really an obvious cyber threat, but it can be used in a hybrid campaign which could affect share prices or sales. The NCSC has tried to combat cyber attacks on the UK electoral system by providing advice to local government and political parties. It also has a role in policing content on the internet.

Additional cyber attack incidents

Here the Threat Report highlights CEO/business email compromise fraud, major security vulnerabilities, financial sector compromise and cyber crime as a service.

CEO/business email compromise fraud

Business email compromise scams are a serious threat to organisations of all sizes and across all sectors, including non-profit organisations and government. The most effective way for hackers to gain a foothold in systems and install keyboard loggers or ransomware is to get people to click on links. This can be done by tricking people into downloading malware infected files, or more commonly by sending people 'phishing emails.' It is one of the fastest growing, lowest cost, highest return cyber crime operations. Action Fraud and the National Fraud Intelligence Bureau operate a 24/7 hotline for businesses to report live cyber attacks.

Major security vulnerabilities

The Spectre and Meltdown vulnerabilities allow programs to read data in programs running elsewhere in the processor, thus leading to potential crucial data leakage. They both execute on personal computers, smartphones, tablets and servers in the cloud. Spectre actually makes it possible to steal data from other customers in the cloud. Meltdown can be patched through software. Spectre however is harder to exploit than Meltdown, but also harder to fix.

The NCSC's mitigations against Meltdown and Spectre include using up to date and supported operating systems, hardware and software, deploying critical security patches as soon as possible and checking the manufacturer of the hardware to see if it has published security updates.

Financial sector compromise

Financial sector organisations are an obvious target for cyber criminals. I am reminded of the bank robber who was asked why he robbed banks. He replied "[...] because that is where the money is." The financial sector has the money. Breaching systems in the financial sector like Citigroup, Zurich or HPE can result in sensational pay outs. Of course, underneath such organisations is a complex digital ecosystem, and much of this critical infrastructure relies on the uninterrupted use of the internet and the communications systems, data, monitoring, and control systems that make up this infrastructure. The Far Eastern International Bank ('FEIB') reported a cyber enabled fraud that had been committed using the SWIFT system. Malware, believed to have been delivered by a spear phishing email, infected the company's IT systems used for the SWIFT payment network.

NCSC's mitigations against financial sector compromise include using up to date and supported operating systems and software, deploying critical security patches as fast as possible, deploying an always-on antivirus solution that scans new files, conducting regular vulnerability scans and action critical results, implementing application whitelisting technologies to prevent malware running on hosts and establishing configuration control and management.

Cyber crime as a service

Cyber crime as a service is a reality that is often driven by organised criminal organisations which are finding new ways to gain unauthorised access to networks, and new methods to profit from that access. They have basically moved to where the money is. These cyber crime units possess roles that we typically come across in any large legitimate business such as partner networks, associates, resellers, and vendors. They even have dedicated call centres which are typically used to help with requests from ransomware victims. Of course, they use sophisticated methods to remain hidden such as encryption, dark web forums, virtual private networks and other obfuscation techniques.

They offer franchises which allow other hackers to replicate their botnets and vectors of compromise. They even provide training. Bitcoin is the preferred currency. This helps them remain hidden from the authorities. They also have global reach. The reFUD.me service allowed offenders to test, for a fee, whether their malicious cyber tools could beat antivirus scanners. The service also sold custom made,

Image: gremlin / iStock / Getty Images Plus / Getty Images Plus

Cyber crime damage is now measured in the trillions annually and is fast becoming the leading criminal damages threat to organisations.

malware disguising products and offered technical support to users. The National Crime Agency worked collaboratively with Trend Micro to form a virtual team designed to find innovative ways to tackle cyber crime threats assisting in the investigation into eFUD.me, which resulted in arrests and the takedown of both reFUD.me and Cryptex.

Future threats

The future threats which were highlighted include data breaches and legislation, cryptojacking, increased use of worms, Internet of Things ('IoT') and cloud security.

Data breaches

Under the General Data Protection Regulation ('GDPR') organisations will have a duty to report to the relevant supervisory authority data breaches which are likely to result in a risk to the rights and freedoms of individuals within 72 hours of the organisation becoming aware of the breach. The true cost of a data breach to an organisation can be difficult to estimate. It can be both under and overestimated. There are some guides to help in estimating the cost which can be sought from previous cyber liability insurance claims. In general, the cost of stolen records is affected by the type of data and total number of records compromised.

Of course, the presence of credit card numbers or medical records can affect this greatly. There is a linear relationship between amount estimated for breach and number of records compromised. Other factors which can affect the costing are whether there was stolen IP, business downtime and damage to brand reputation. These can all be significant cost adjustors in the final estimation. In fact, the true cost can only really be gauged years after the breach. Time will reflect a more realistic data breach cost estimation. The NCSC expects to see an increase in the number of reported cyber incidents.

Cryptojacking

The technique of delivering cryptocurrency miners through malware which uses an individual's computer processing power to mine cryptocurrency without their consent is on the rise. Check Point reported that 55% of businesses globally were impacted by cryptominers. These include popular websites. The primary way users may notice their devices are being cryptojacked is a slight slowdown in performance. Using an adblocker or antivirus programme which have features that block browser mining is the best way at present to prevent this.

Internet of Things

The buzz around IoT has been noticeable for several years and the potential of the technology is undeniable. A variety of devices are now being connected to the internet, from fridges to GPS trackers on wild animals, all of which are offering numerous benefits. There are however serious security concerns and in our rush to bring the technology to the mainstream, a key step has been missed that could lead to IoT being brought to its knees. IoT has been developed at such speed that security standards have failed to be developed at a similar pace. Recent cyber attacks, such as NotPetya and WannaCry, have crippled entire organisations and highlighted the dangers and potential scale of a major breach. The NCSC recommend avoiding default passwords, implementing a vulnerability disclosure policy and ensuring device software can be patched to guide against poor IoT deployment.

Cloud security

Only 40% of all data stored in the cloud is access secured, although the majority of companies report they are concerned about encryption and security of data in the cloud. The cloud can also relieve businesses of the need to implement burdensome disaster recovery plans, as cloud providers take responsibility for implementing backups and maintaining a live stable environment. There are also many savings to be made for large businesses when performing maintenance, especially with regard to updates, as the provider can roll these out. This aspect alone makes cloud computing an attractive option. However, the Threat Report states that hackers will take advantage of the fact that many businesses put too much faith in the cloud providers and do not stipulate how and where their data is stored. This could lead to further breaches involving UK citizen information.

Conclusion

Organisations need to be aware of the need to invest in security. The areas that require investment will differ between organisations but ultimately, it needs to involve all staff in efforts to remain secure. This is because the actual technology is only part of the equation. Humans are generally the weakest part. Education is a large part of it. We must be aware that phishing emails are still the number one vector of compromise. Security professionals know many of the risks at present, but getting management buy-in can still be difficult. The risks include collection of data - due to the growth in the volume, variety and concentration of data, this is a high value target. Increased sharing of data also increases vulnerabilities by widening the attack surface. The attacks are indeed becoming more sophisticated. As we say in the cyber security business, attacks always improve over time. Companies also now risk huge fines under the GDPR.

Of course, a large part of cyber crime is driven by organised criminal organisations which are finding new ways to gain unauthorised access to networks and new methods to profit from that access. They recruit based on aptitude, technical and criminal expertise, and are even patient with members learning on the job. Cyber crime has truly become an industry, and UK companies are a target. Threat reports like this are welcome.