SECURITY+

Is yOur dAta beinG HeLd to RaNsOM?

COMBATING THE INSIDER THREAT

4 VITAL STEPS TO DEFEND YOUR NETWORK

UNDERSTANDING GDPR AND THE SNOOPER'S CHARTER

HOW CYBER ESSENTIALS CAN PROTECT YOUR BUSINESS

e92plus

Welcome to

SECURITY+ MAGAZINE

The security threat landscape is always changing, but there are key challenges that organisations are currently facing.

In this issue we discuss the introduction of the EU GDPR, and what you can do to ensure your organisation is fully compliant. We also speak to one of the authors of Cyber Essentials, the security framework that is becoming a must for organisations of every size.

We also look into the threat of ransomware, what you can do to protect your data from being held to ransom, the dangers of an unprotected Wi-Fi service to a business, and understanding that threats to your data can come from both outside and inside the company.

As ever, we welcome your feedback - so if you have any questions or would like more information on the articles or threats featured, please get in touch at securityplus@e92plus.com.

CLAIM YOUR FREE PERSONAL SECURITY LICENCE!

To help keep all of our readers secure, and their family protected, we are offering everyone a free personal home security licence to cover their desktop, laptop and mobile devices.

This exclusive offer, in partnership with Bitdefender and Trend Micro, is available to claim today at www.securityplusonline.co.uk/free

Bitdefender

TREND MICRO

WIN A FREE EMPLOYEE CYBER SECURITY AWARENESS DAY!

This issue of Security+ explores many solutions to the threats to our networks, but the biggest threat is our users - and the most powerful defence is education.

That's why we are offering a free Employee Cyber Security Awareness Day to one of our readers. We'll provide an essential introduction to the modern network, insights into the latest threats and most importantly practical tips for staying safe and secure at work.

For your chance to win, simply visit www.securityplusonline.co.uk/awareness

INSIDE THIS EDITION

COULD THE SNOOPER'S CHARTER OPEN THE FLOODGATES FOR ONLINE EXTORTION?

By Raimond Genes,
CTO at Trend Micro

We have seen online extortion manifest in the ransomware epidemic which has seen those behind CryptoWall net hundreds of millions. Why exactly will we see more and more hackers demanding money from firms not to release customer data they've stolen? After all, it's always been the case that a major breach can lead to prohibitive clean-up and remediation costs, industry fines, possible legal fees and reputation damage. Well, the hackers are getting cleverer and the tools to launch such attacks are increasingly widespread on the cybercrime underground. But more than that, it's becoming less and less financially rewarding to target individuals.

If you're running Windows 10, for example, you'll have to click through several warnings to download most ransomware. Even Windows 7 has safeguards built in – so fewer are doing so. Then we've got the think about the multiplicity of operating systems out there. If an attacker sends out a piece of ransomware, no matter how neatly crafted it is there is now a growing percentage of the population who won't open it on the Windows PC it was designed for but a tablet, or a smartphone. In short, the addressable market is waning.

That's not to say ransomware and other online extortion isn't still happening. Of course it is. But the prospect of hacking a major corporation and obtaining thousands or millions of customer records becomes that much more attractive.

And the more TalkTalk-type stories there are in the headlines, the more hackers prick up their ears. There'll be many out there right now inspired – thinking if it were them, they'd have done it better.

Snooper's Charter: Danger Ahead

While we're on the subject of extortion, several reports have suggested recently that internet users' browsing history could be the next major source of online blackmail for hackers in the wake of the Ashley Madison attack. Rest easy netizens: there's not much chance a cybercriminal is likely to go to the effort of targeting an individual, working out their name and circumstances and then crafting an online extortion plot. But there is danger ahead.

If the proposed Investigatory Powers Bill is passed in its current form then I fear the worst. It requires ISPs to retain the web history of everyone in the UK for 12 months. These massive data stores would be an incredibly attractive target for online extortionists. Home secretary Theresa May has claimed that these records will not include the individual pages of a site a user visits, but a site address alone could be enough for a blackmailer. The government must make sure if this law is passed that it mandates the highest data security standards for the ISPs tasked with following it. However, as we see with each passing breach of customer data by a big name organisation (JPMorgan anyone?) – even those firms which spend millions on security can be hacked by a determined adversary. Someone will almost certainly try to hack these records, and eventually someone will succeed.

Bring in the DPOs

So what can these firms do to minimise the risk of a damaging breach? Well, follow the basics for sure. Enforce strong two-factor authentication, reduce the number of privileged users to the bare minimum and operate an access policy of least privilege. You also need good visibility into what's going on inside your network. If it was breached via a simple SQLi, TalkTalk should have been able to spot and block the huge number of customer records flowing out to an individual IP address. Systems also need to be patched and up-to-date to minimise the chances of any software flaws being exploited. And remember to regularly pen test systems to ensure they're as secure as they can be.

But perhaps the most important step from an organisational perspective is to appoint a Data Protection Officer (DPO). We predict that by the end of next year less than 50% of organisations will have one, despite it being a requirement of the forthcoming European General Data Protection Regulation. Unlike a CISO, the DPO has a role specifically focused on protecting the organisation's most important resource – its data. And even better – they are independent of the IT department and can't be fired as easily by the CEO.

In short, they occupy as objective, dispassionate and critical a role in improving data security within an organisation as you can get. The sooner more firms realise this, the more secure all of our data will be.

TREND MICRO

4 VITAL STEPS FOR NAVIGATING TODAY'S SECURITY THREAT LANDSCAPE

By Matthew Walker, VP Northern Europe at HEAT Software

IT security is no longer just of concern to IT security professionals and the CISO today, everyone at the board level, from the CEO, CFO and CIO needs to improve their understanding of and the scale of the problem at hand. Those that don't understand the impact a data breach can have, be it on the service desk or network availability, risk the blame falling at their door should the worst happen.

In recent times the number of software vulnerabilities, as well as the malware being created to exploit them, has exploded. More than 7,000 new vulnerabilities were published last year with software applications widely used within corporate environments such as Adobe Reader and Oracle Java JRE among those that are most affected. In addition, more than 16 million different malware signatures were identified to exploit them.

In isolation, prevention strategies such as blacklisting and antivirus simply can't keep up. The reality is that organisations of all sizes must now build their plans around when, not if, they suffer an attack.

"We not only have a legal responsibility, but also an ethical and moral responsibility to consumers"

Steve Wright, Global Privacy Officer, Unilever at the London SC Congress

1 ENDPOINT SECURITY–DETECT AND RESPOND

Unfortunately, it's simply not possible to lock down IT like it used to be. Gone are the days when the IT department had absolute control over which applications were allowed to run on the network. In an era of mobile working, cloud computing, Bring Your Own Device (BYOD) and the Internet of Things, no organisation could accommodate that level of inflexibility. With each passing month we see new examples of the limitations of the traditional IT security technologies and toolsets in eradicating new threats. Where antivirus was once the pinnacle of IT security, most organisations today see it as little more than a single piece of a thousand piece jigsaw puzzle.

In response, virtually all organisations are recognising the need to adopt a 'detect and respond' mentality in order to get back on the front foot. Indeed, the 2016 Ultimate Windows Security threat landscape survey found that discovery and analysis was the top security priority for the 700 IT professional respondents worldwide.

There is no magic bullet solution but fortunately 99% of risks can still be eliminated by regularly and consistently applying simple security precautions. Indeed, narrowing risk exposure to one percent is a realistic and hugely important goal for any CIO who has not already done so. Specific strategies can then be deployed to detect, respond and mitigate against the impact of more sophisticated attacks.
The first and most important step is understanding which endpoints are connecting to the network and which software applications are being allowed to run. Only then is it possible for security teams to enforce the kinds of systems and policies that ensure strong levels of security.

For example, despite years of warnings about clicking on suspicious emails and websites, users still regularly fall prey to them. According to a study by Verizon, nearly one-quarter of email recipients open phishing messages and 11% click on phishing attachments. Or to put it another way, a campaign of just 10% success has a greater than 90% chance of installing malware on a user's PC.

Giving IT and security teams the ability to detect and respond to what is already present in the network is therefore equally, if not more important, than the measures taken to prevent threats from being introduced. Firstly, so that they can ensure all users understand the risks, as well as their responsibilities in helping to protect corporate information. Secondly, so that they can implement a well-developed reaction plan to enable rapid containment and recovery should a data breach occur.

2 CREATING A LAYERED APPROACH

The most effective defence has many layers but begins with intelligent whitelisting. Security policies such as antivirus have, in recent years, proved the limitations of blacklisting – the security threat landscape is simply too big and hackers, too smart. A whitelist approach

to application control is much more effective, beginning with a local list of approved software applications, alongside a trust engine that lets IT define criteria for trusted applications.

For example, IT can specify trusted publishers, updaters, paths or locations. It also lets them maintain a blacklist of denied applications that for security, productivity or even bandwidth usage reasons users are unable to introduce into your environment. This means even if software that isn't explicitly on an organisation's whitelist does end up on its machines, it simply won't run. Combine this with regular and consistent patch management and CIOs can rest assured that their organisation is protected against all software vulnerabilities that are already known to the major software vendors such as Google, Apple and Microsoft.

These routine steps of introducing application control and regularly patching all trusted programmes can eliminate 99% of the IT security risks to the organisation. However, user education, antivirus, device control and configuration management all have a role to play in providing a well-rounded and robust defence of IT networks. Realistically, no organisation will ever get to 100% secure, but this approach prevents the final one percent being a catastrophic gap.

3 TACKLING RANSOMWARE

Ransomware has been dubbed the fastest growing 'industry' in IT security, affecting big and small businesses alike, in every industry. Crypto-ransomware, in particular, is an insidious and rapidly emerging technique which uses strong cryptography to encrypt all data stored locally and directly attached to a server or workstation, holding it hostage until the ransom payment is made.

Unlike more targeted attacks or malware with espionage-related goals, ransomware is opportunistic and generally not targeted at any specific individual or organisation. Typically delivered via phishing emails, drive-by downloads, or malvertising, anyone with an email address or a web browser is a potential victim.

Patch management remains one of the most effective means of thwarting attacks, including crypto-ransomware. Essentially, patching reduces the known software or network vulnerabilities to minimise the exploitable areas attractive to cyber criminals. To protect against crypto-ransomware in particular, patching operating systems, Microsoft Office, Adobe applications, web browsers and browser plug-ins are important. To that end, centralised patch management is key. Without a centralised solution, businesses are left to rely on multiple individual updates from every software vendor, which becomes impossible to manage. Additionally, devices and network performance can become degraded, and if users are turning off auto-updates, a business' exposure to risk becomes far greater.

4 CONNECTING SECURITY AND THE SERVICE DESK

A key step towards coping with increasing security risks is ensuring that the business is equipped to communicate, manage and resolve incidents with utmost efficiency. This can only come by achieving harmony between security and service desk teams. The benefits of better collaboration between these teams is perhaps nowhere more keenly felt than in terms of BYOD. By 2018, Gartner predicts that 40% of contact with the IT service desk will be related to smartphones and tablet devices, an increase from less than 20% in 2015. Threats like ransomware, which are increasingly targeting mobile devices, will drive this increase and, as companies introduce BYOD strategies, they need to ensure that these personal devices are secure to access the network and, in doing so, bringing the service desk and security together is essential. At the most basic level, you can't properly manage devices without accounting for security and you can't secure them without managing them.

IT security and service desk collaboration is just as important for company-wide policies as it is for each individual device. For instance, the process of introducing cloud apps like Dropbox at a company-wide level will have a profound impact on the service desk and IT security team alike. The service desk will need to implement new processes and will need to expect a spike in support requests before, during and after migration as employees acclimatise to new processes. Likewise, IT security needs to get used to the idea of confidential files being stored in the cloud and not on premise, while ensuring the same level of security.

"The biggest (endpoint risk) identified in this year's research is the negligent or careless employee with multiple mobile devices using commercial cloud apps and working outside the office"

2015 State of the Endpoint Report: User-Centric Risk, The Ponemon Institute

"The status quo is no longer fully effective for endpoint security.

Application control, when used as part of a multi-layered approach to endpoint security, shows great promise in the enterprise battle against sophisticated malware and unwanted applications."

Derek Brink, Vice President and Research Fellow for IT Security, Aberdeen Group

The security threat landscape is complex, multi-faceted and ever evolving. However, IT and security teams can prevent, detect and respond given access to the right technologies and toolsets. This is the CIO's responsibility as much as anyone in the business, and the time to take action is now. It is a question of when, not if, businesses are subject to attack. Therefore creating rules and a layered approach to security before an attack is any organisation's best chance of staying secure.

HEAT software

Learn more about key endpoint strategies with HEAT Software at www.securityplusonline.co.uk/HEAT

CELEBS, CORPORATIONS & CONSUMERS

EVERYONE CAN BE A CYBER VICTIM

By Liviu Arsene, Senior E-Threat Analyst at Bitdefender

Cybersecurity has become a major topic of discussion for businesses and organisations of all sizes, as the number of security incidents has spiked, capturing headlines worldwide. This year, even presidential candidates and campaigns will likely join the discussion, as 64% of registered U.S. voters believe cyberattacks will undoubtedly plague election campaigns, according to a study from Experian.

If until now the cybersecurity landscape was somewhat uniformly distributed between activism and public shaming, today's cyberattacks are either financially motivated or state-sponsored, and aim to steal state secrets or cripple critical infrastructure. Politically motivated cyber-attacks seem to have been at the heart of the Ukraine cyberattack on its power grid during the Russian-sponsored conflict there in late 2015.

Cyberattacks Can Hit Anyone and Anything

Even if they're targeting a government or private organisation, cyberattacks can hit individuals, especially public figures, celebrities or otherwise politically engaged people. The "Celebgate" iCloud leak is a notorious example from 2014 when more than 500 private and nude pictures of celebrities were leaked to the internet in one the most controversial phishing scams in the past couple of years. With social engineering at the heart of it, the incident prompted a massive investigation fallout and public debate on whether people should even be looking at the pictures and urging authorities to apprehend the cybercriminal.

A more recent attack on an individual's public image has to do with Anonymous declaring "war" on Donald Trump, one of the candidates for the Republican nomination for President of the United States in the 2016 election. The hacker group openly started a campaign against Trump, threatening to find and post all personal and sensitive information they can find on him.

"The single biggest existential threat that's out there, I think, is cyber"

Michael Mullen,
retired United States Navy Admiral

Hospitals have also been the target of malware – particularly ransomware. In February 2016, the 434-bed Hollywood Presbyterian Medical Center stated they had to pay the equivalent of $17,000 in bitcoins, to hackers who seized their computers and encrypted all data on them. While at first the cybercriminals demanded $3.4 million to restore access to the hospital's computers, a negotiation took place to release them for a smaller amount.

Even operating systems believed less susceptible to malware have been kneeled by ransomware attacks. Linux was the one to be hit by Linux.Encoder – the Linux version of the ransomware threat – in late 2015, and in early March 2016 Apple OS X was targeted. The unprecedented Mac ransomware threat is believed to have affected thousands of users, as the infected application was estimated to have been downloaded by more than 6,000 users.

While the Linux variant was relatively easy to crack, as security researchers were able to provide a tool to offer free decryption of the infected files, it stands to reason that cybercriminals will improve the threat to make it more difficult – even impossible – for the researchers to decrypt the files.

How Can Businesses Protect Themselves?

Probably one of the first things organisations need is a policy for enforcing strong authentication methods, particularly strong passwords for all users. According to a 2016 study from SplashData, the two most popular passwords for the past couple of years have remained "12345" and "password," while the third is "12345678". While most data breaches that affect companies involve stealing employee credentials via phishing or social engineering scams, attackers have been able to breach particular networks just by guessing or brute -forcing authentication credentials.

Another important security measure that organisations need to implement is endpoint security and some form of centralised security management console that can offer security administrators visibility into network threats and the capability of remotely managing security policies. Combining that with network traffic monitoring capabilities, organisations can actively watch their infrastructure for threats and intrusions.

Companies that accept BYOD should have the proper policies set in place to avoid data or network breaches caused by infected employee devices connected to the corporate network. To this end, organisations that decide to support BYOD should start setting up DMZs, separate networks for employee personal devices, and even specify which devices are permitted to access – or not – critical data.

CIOs are also encouraged to start looking for a penetration testing and vulnerability scanning team or solution that's able to constantly stress-test the internal infrastructure and come up with new plausible attack scenarios to help train both employees and the IT department. This has been considered a very effective tactic in proactively fending off cyberattacks and in minimising the financial impact of a security breach. CIOs and CSOs need to budget these security assets and convince upper level managers that the benefits of having such a team far outweigh the financial risks they're exposing themselves to.

Of course, in the security chain the weakest link is usually the human component, which is susceptible to social engineering, phishing and other forms of cyberattacks. To this end, educating all employees in identifying threats or fraud attempts and reporting them to internal IT departments is mandatory. Some of the most prone to spear phishing attacks or spam campaigns are usually personnel in accounting, human resources, or acquisitions, as most email usually contain titles related to "please check attached invoice," "here's your confirmation order," or other such topics.

Finally, one crucial thing that any organisation or company needs to prepare is a worst-case-scenario. These are designed to quickly identify key stakeholders in case of an eventual data breach, personnel responsible to mitigating the found threat or vulnerability, how and when to start communicating with your customers if their data has been compromised, and a forensic team that can study the breach thoroughly to quickly come up with ways to prevent such future cyberattacks. After a security breach, all companies need to ask themselves what they have learned from it. If the answer doesn't immediately translate into actions or steps taken to proactive counter similar such attacks, a similar attack is bound to happen again.

It's all about the money!

Whether its companies or cybercriminals, the main motivation behind either setting up corporate security mechanisms or developing malware is always money. When allocating or forecasting security budgets, companies usually rely on the CIO and CSOs to perform SWAT analyses and risk assessment strategies to convince the stakeholders to share a bigger slice of the "cash" budget towards security. At the other end, malware coders usually apply the same strategy when writing malware, as their main focus is to either steal and sell intellectual property or extort their victims.

The main difference between security and cybercriminals is that the return-on-investment for deploying security technologies within an organisation is far smaller than the one for cybercriminals. For ransomware alone it has been estimated that the ROI is around 1,425%, according to a security report. To this end, it's safe to assume that, while companies might find it difficult to justify additional security costs either on a quarterly or yearly basis, cybercriminals are in the win, as they're getting the most benefit with minimum investment.

"A cyber hacker is nothing more than a bank robber using another weapon. His motivation is robbery and theft."
L. Collins

Amid the proliferation of IoT devices and their integration with corporate networks, Gartner believes that security costs will increase to 20% of annual security budgets. Ironically, the malware-as-a-service industry will start reducing development and deployment costs as new tools are being developed that make it amazingly simple even for non-tech-savvy individuals to purchase, customise and deploy threats on a global scale.

Takeaway

While security experts have been arguing that large, medium and small businesses need to stop thinking about "how" and start thinking of "when" they're going to be breached, it's up to CIOs and CSOs to both prepare for the worst and disseminate this message to all company stakeholders.

What is increasingly clear is that cybercriminals will up the game in performing cyberattacks, and companies need to be prepared to fight – and sometimes lose a battle or two – against this wide range of potential cyberattacks. The challenge here is to always learn from past mistakes and collaborate with both government institutions and private security companies in fending off, mitigating and recovering from future attacks.

Connecting the APT Dots

Advanced persistent threats (APTs) are attacks against targeted companies and resources. Typically, a social engineering attack on an employee triggers a series of activities that opens up the company to serious risks.

6 STAGES OF AN APT

Acquire strategic information about the target's IT environment and organizational structure

INTELLIGENCE GATHERING

31% **of employers subject employees** who post confidential company data on social networking sites to **disciplinary action.**

Gain entry into a target's network via email, instant messaging, social networking, or software exploitation

POINT OF ENTRY

In an experiment, **87%** of organizations clicked a link **related to a social engineering lure.**

Ensure continued communication between the compromised host and the C&C server

COMMAND-AND-CONTROL (C&C) COMMUNICATION

Major APT campaigns use **web ports to communicate** with C&C servers.

Seek valuable hosts that house sensitive information within the target's network

LATERAL MOVEMENT

The techniques used include passing the hash, **which elevates an attacker's privileges to that of an administrator,** allowing him to gain access to key targets like mail servers.

Identify valuable data to isolate for future data exfiltration

ASSET/DATA DISCOVERY

Company secrets comprise **2/3 of enterprises' information portfolios though only half** of their security budgets are devoted to protecting these.

Transmit data to a location that the threat actors control

DATA EXFILTRATION

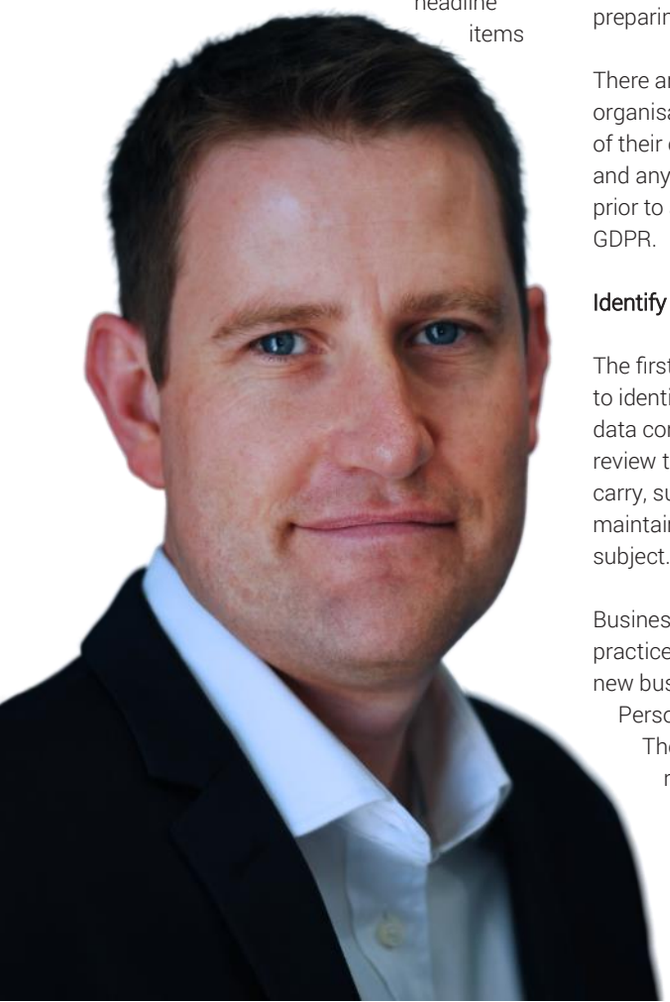
SONY SPENT MORE THAN US$171M AND **RSA** spent US$66M to undo the damage brought about by **data exfiltration from its network.**

KEEP YOUR FRIENDS CLOSE... BUT YOUR INSIDERS CLOSER

By Neil Thacker, Information Security & Strategy Officer EMEA at Forcepoint

The clock is officially ticking for organisations to get their data protection policies in order, now that the General Data Protection Regulation has been approved and is set to replace the previous EU Data Protection Directive.

The new regulation will come into effect in 2018 and will require businesses to put a much stricter focus on data protection. The headline items for organisations that collect or process EU citizen records are:



- They must notify their supervisory authority of a data breach within 72 hours.
- The subject will have the right to retract consent, request data erasure or portability.
- They may face fines of up to 4% of their worldwide turnover, or €20 million for intentional or negligent violations.

These increased sanctions mean it is vital that this new law be fully understood by a number of key stakeholders within the organisation, and that organisations start preparing as soon as possible.

There are five key steps to help organisations perform a basic assessment of their current data protection strategy and any potential gaps that need filling prior to a more comprehensive view of the GDPR.

Identify

The first task for any organisation must be to identify whether they are considered a data controller or processor. They must review the relevant obligations that these carry, such as issuing notice to citizens and maintaining relevant consent from the data subject.

Businesses should make it common practice to regularly review existing and new business processes to identify Personal Identifiable Information (PII). They should identify where this data resides – whether it is at-rest, in-motion and/or in-use and maintain a record of processing activities and understand how this data is protected.

Protect

Once PII has been identified, organisations must then ensure they adequately protect this data. Encryption and access control are common control standards, but managing encrypted data across multiple business processes is a difficult task.

Data sovereignty and data lifecycle management are key to helping businesses ensure that EU citizen data is processed and stored appropriately. In addition to this, they also need to manage data flows to approved third party processors, monitor for accidental data leakage from negligent or malicious employees and protect against data theft from external agents.

Detect

If an organisation does suffer a loss of data then it is vital to detect the breach and identify if PII records were lost or stolen. If they have, the business will be required to notify the necessary authorities within 72 hours of the discovery to initiate a full investigation.

The investigation will focus on identifying the source and destination of the breach through event and incident information from Data Leakage Prevention (DLP) and Data Theft Prevention (DTP) tools. Data forensics will then help to pinpoint the stolen data, at which time the business will be required to issue notice to any affected data subjects.

FORCEPOINT
POWERED BY Raytheon

HIDE AND SEEK: HOW TO AVOID THE ATTRIBUTION TRAP

The almost endless stream of high-end data breaches affecting some of the world's biggest organisations in the last 18 months highlights the fact that no business is safe from being hacked. From the massive data breach suffered by Target to the high profile leak of Ashley Madison members' details, it's clear that every business has to be aware of the latest threats they face from cybercriminals.

We are seeing a surprising shift to attack activity on commercial targets that exhibit characteristics typically observed in nation-state related attacks that aim to disturb economies, disrupt consumer confidence and drive political agendas. For example, health insurance provider Anthem found its name making headlines for all the wrong reasons after cybercriminals stole information on tens of millions of its customers.

Attackers are increasingly going out of their way to disguise their origins, methods and sources to gain access to their desired data, with the most popular methods observed:

- Breaking the chain of traceability through the use of the free software TOR (The Onion Router), which hides location or browsing information.
- Using compromised websites that have been registered by an unrelated third-party.
- Using hosting providers that refuse to cooperate with abuse notifications or law enforcement requests.
- Creating a complex series of redirect chains, which function for a single use.
- Recycling codes, meaning it's unlikely that the attacker is the author, or inserting misleading strings, web addresses and code paths into malicious binary files.
- Obscuring DNS paths by using frequently changing IP addresses.

The natural reaction for many businesses in the wake of an attack is to seek out who has gone to the huge effort to attack them on such a scale. However, it is particularly difficult to assign attribution correctly given the ease with which hackers can spoof information, circumvent logging and tracking or otherwise remain anonymous, as outlined earlier.

Rather than being fixated on chasing down the hacker, companies should instead be focusing their attentions on the tools, techniques and procedures of their adversary (TTP). This gives businesses a better chance of defeating the next attack or attacker that uses a combination of the same TTP – especially as malware authors share TTP. Businesses that suspect they are dealing with a nation-state attack could in fact be dealing with a much more junior attacker that has simply acquired tools previously used by nation-state actors.

The need to improve security defences to learn from previous failures and address possible future attacks has to be a high priority that should be taken up appropriately by the IT team, while working with professional investigators with the necessary skills and resources.

Businesses should focus on a forensic investigation that profiles the attacker, but only to the extent of understanding their intent and techniques. They can then adjust their defences and processes to maintain an adaptive security approach.

Having the right balance between their priorities will maximise IT's contribution to the organisation and ensure the business is appropriately prepared for future attacks. Businesses must ensure they do not get distracted by chasing attribution breadcrumbs, but instead focus their limited resources on threat prevention and remediation.

Response

Incident response is critical to protecting confidential and EU citizen data. In addition to the mandatory data breach notification requirement, organisations must also ensure they have implemented an effective incident response plan. This plan must have been tested to ensure that employees involved in a data breach response are familiar with and fully understand the new legislation and communication process in order to report a breach.

Recovery

In the aftermath of a data breach businesses must ensure they maintain ongoing communication with the relevant authorities. This will ensure secondary loss factors are managed and keep affected data subjects regularly informed.

Data protection and the safeguarding of EU citizen data has always been an important requirement for organisations, and the impending GDPR places even greater emphasis on the value of this data. It is therefore more important than ever for organisations to fully understand their role and apply the appropriate security controls that allow them to identify and protect this data. Having an established data breach plan in place will then help organisations be familiar with the detect, response and recovery phases to ensure they limit the effect of the attack and have the relevant people, process and technology in place to continually deal with this new legal requirement.

For more information, you can view our video on the Insider Threat at **www.securityplusonline.co.uk**

A QUICK WIN IN THE FIGHT AGAINST DATA THEFT

For all the disruption they caused at the time, the hack attacks on TalkTalk, Target, Ashley Madison, and JD Wetherspoon in the latter half of 2015 have focused executives' minds on cyber risks like never before. In the aftermath, the brands affected were falling over each other to explain the steps they were taking to ensure they it never happened again. Investments in cyber security – often viewed as an expensive overhead – were suddenly a source of pride; hitherto onerous data protection regulations became a safe refuge in the face of increasing public scrutiny.

This is very encouraging, but the concern is that their focus is too far-sighted. There is a grave danger that organisations are channelling resources towards mitigating external threats, while neglecting the risks that come from within. The dangers of this became clear in February, when a former employee of Ofcom was caught attempting to pass confidential data to his new employers. That the data was passed to another business and not to a 'dark net' download site is immaterial – sensitive information was compromised, as a consequence of which Ofcom found itself apologising to the broadcasters and media organisations it's meant to police. Unfortunately, Ofcom's case is by no means isolated.

Like external threats, organisations' approaches to mitigating internal risks have been patchy, with overzealousness in some areas masking lassitude elsewhere. Most firms, for example, have rigorous password protocols. However, how many continually adjust and refine employees' access to applications and data as their roles change – so people only have access to what their job requires?

Manage the endpoints, and the risks will manage themselves

This patchwork leads to a confusing mass of information and intelligence - which makes building a clear picture of the organisation's security posture and vulnerabilities difficult and time-consuming. In a world where data from a stolen device could be somewhere for sale within minutes, the ability to monitor – and act – in real-time is crucial. To put it another way, organisations must build a 'single source of truth' covering all of their end-points including desktops, laptops, smartphones and tablets.

Mitigating internal threats in this environment revolves around the ability to do three things very well:

1. **Account for the location of employer-owned devices** - offering flexible working carries with it the implicit trust that employees will safeguard their devices and data. Endpoint security technology can add a further layer of reassurance, by tracking the location of devices and sounding the alarm if they travel outside a given perimeter and allowing action should the device be lost or stolen.
2. **Detect and mitigate suspicious behaviour** – as night follows day, attempts to circumvent corporate IT security technologies by an employee (such as disabling the anti-virus) are indicators that the user plans to take their device beyond 'acceptable use'. In these circumstances, administrators need to monitor and manage end users and their devices in real-time - which could mean deleting data, disabling the whole device, pushing out updates or turning on encryption.
3. **Provide a thorough audit trail** – data is everything when organisations are reassuring staff and customers after a security breach. What is more, regulators increasingly demand it - and compiling a detailed narrative could be essential for both forensic and reputational reasons.

Broader benefits

There's more to endpoint security than tracking down errant data and catching out careless staff. The single source of truth on endpoints can start paying for itself almost immediately, in the form of improved IT asset management. Organisations have long been paying for more software licences than they actually need to avoid potential fines. Security tools can be manage that, avoiding unnecessary purchases and easily re-allocating the licencing when they are no longer needed.

Intelligence is everything

If there is one lesson from the security breaches of the past year, it is that nobody can consider themselves immune to attack. While external threats are more challenging to mitigate (as well as generating more column inches), the actions of staff within the organisation are just as dangerous - whether through deliberate data or device theft, or simple mistakes or ignorance. By building a single source of the truth about the status, location and content of their devices, IT teams will chalk up a quick win for ensuring the unthinkable doesn't happen for some time to come.

THE INSECURITIES THAT HAUNT PUBLIC WI-FI

By Perry Correll,
Principal Technologist, Xirrus

It's no surprise to anyone that Wi-Fi use continues to grow. However, what is hard to believe is that there are so few public Wi-Fi networks capable of serving our needs outside of the home securely—particularly when you consider that as of today, nearly everyone owns a smart phone, 91% use a laptop, and 80% have a tablet. The portability of these items reflects intent of use, which is, of course, mobility. But there is little point in being able to work remotely from a coffee shop, do banking from our phones while waiting at the airport, or make purchases from the comfort of a hotel room when there's a high risk of having data stolen due to the lack of security when using public Wi-Fi.

Xirrus recently polled Wi-Fi users and found that 76% connect to Wi-Fi outside of their home. With the proliferation of wearable devices such as fit bands and smart watches, that figure will only increase with each passing year, thereby presenting additional temptations for hackers. Public Wi-Fi offers the convenience of accessibility, but typically doesn't encrypt data, which leaves passwords exposed and sensitive data vulnerable to the possibility of capture by those with malicious intentions.

It's bad enough worrying that while sipping a latte, cyber criminals might be trying to steal your credit card data and bank account numbers, but even more daunting to know that corporate espionage is on the rise. Hotel Wi-Fi networks, which are notoriously easy to breach, offer hackers little challenge when it comes to intercepting private or classified information accessed by executives who stay in hotels on business.

Now more than ever, large and small enterprises—from coffee houses to airports and hotels—must upgrade their networks to provide better security for their customers.

Stay secure on public Wi-Fi

We offer a few tips on how you can use public Wi-Fi and maintain some level of security:

1. When connecting to public networks, be careful to ensure the SSID name and method of encryption are exactly as advertised by the provider.

76% OF USERS THINK PUBLIC WI-FI IS NOT SECURE....

...BUT 62% STILL USE IT

2. Do not enter credit card details or other personal information on the provider's network unless you are using an SSL or VPN. Ideally, use vouchers or other information when possible (such as name/room number in a hotel setting). When in doubt, call the provider's support number and validate the method of connection.
3. Public networks should have device-to-device communications turned off. If you can see other users on the network through, say, AirDrop, Finder or Explorer, disconnect immediately. This Wi-Fi network has a security hole.
4. Check the public IP address of the network (you can do this with mxtoolbox.com) and verify the DNS name to ensure it is in fact the provider's network.
5. If you want to access sensitive websites – banks, financial institutions, corporate servers, etc. – make sure to run your VPN software in full tunnel mode. Check with your IT department if you don't know what this means.
6. When it comes to open networks, either never connect, or delete open networks immediately after you've used them. Hackers widely use open networks to collect personal info, or worse, to execute a distributed denial of service (DDoS) attack against a mobile device, with the aim of crashing an app and/or possibly the OS. This kind of attack can render the device unusable.
7. If ever in doubt, disconnect, and do not reconnect to the network.

XIRRUS
WI-FI NETWORKS

www.securityplusonline.co.uk/xirrus

YOUR WI-FI BUT THEIR USAGE: WHOSE RESPONSIBILITY?

In today's world, wireless connectivity is ubiquitous. Universities, enterprises, large public venues (stadiums, shopping malls, airports), hotels, points of sale, healthcare institutions and smart cities are examples of places where, today, accessing Wi-Fi has become commonplace in serving users on the lookout for an always-on experience. With the will of the EU to harmonize Data Protection across Europe, any business providing Wi-Fi will have to make some changes in the way they are providing Wi-Fi to their customers or users.

What is the EU data protection regulation?

Earlier this year, the European Commission communicated a first draft of the future European Data Protection Regulation to replace the previous Data Protection Directive. The goal of this law is to harmonise Data Protection Regulation across the EU countries and it will be directly applicable to all EU member states without going through the process of implementing national legislation.

This will mean big changes to come for any European venues or organisations that offer access to the Internet, as well as for their providers who handle the data and traffic on their networks.

Ultimately, it means that any organisation will be responsible for what is done on their network. This means that they will have to monitor the use of their network in terms of connections and also ensure they will have to provide a secure network to prevent any data breach.

Whatever your business, you will need to protect your network users from data breaches and comply with the law.

With the new regulation, any business will have to cope with IT problems whether they have an IT team (their own or outsourced) on site or not.

Security becomes imperative

Building a wireless infrastructure that not only meets fast connectivity and performance requirements but also addresses security concerns is attainable by focusing on some simple questions.

1. Who is connected to the network?

Being able to identify who is using the next-door restaurant Wi-Fi seems at first easy - and it can be if a captive portal is in use. Providing user authentication means that the venue gets at least the MAC address of the connected device. Not all, but many guest access solutions incorporate a full server for authentication, which checks user identities. Authentication by the web portal is particularly suited to visitors through its ease of use, and providing continual engagement for repeat visitors (via social accounts when logging in, targeted splash pages and geo-tagged promotions & communications) increases visibility.

> *"The customer does not have to worry about the 2006 decree and other legal constraints. **We take responsibility for managing court applications for our customers."***
>
> Dan Michel, Head of the networks and security Business Unit at Diademys.

2. Who can access to what?

Rigorous management of access rights is the key to answer that question. Each user is characterised by his/her profile, which accurately describes the user's rights (Internet connectivity, messaging, and applications). The profiles are applied dynamically during user connection periods, and apply equally to guests, BYOD users and corporate devices.

It also helps to include web security, as filtering can be applied at user profile level. Several URL categories are available (Adult, Aggressive, etc.) allowing different policies, which can be assigned to different profiles (age, employee/guest, territory, etc.). Providers are also responsible for the sites that visitors access, so this filtering is essential to protect the host.

3. What about the obligation to store connection data?

As soon as an organisation provides guest access, it has a legal obligation to keep connection data for those guests who connect to the network. Session logs (who is connected and when?) and activity logs (who did what?), are an indispensable mechanism for meeting the legal requirements laid down by law.

To learn more about how to provide secure connectivity and on-boarding while increasing customer engagement, request your free demonstration today.

UCOPIA
TURN YOUR WI-FI UP

www.securityplusonline.co.uk/ucopia

5 STEPS TO PREPARE FOR THE NEW EU DATA LEGISLATION

The clock is officially ticking for organisations to get their data protection policies in order, now that the final draft and approved text have been made available for the General Data Protection Regulation to replace the existing EU Data Protection Directive.

The new regulation will come into effect in 2017 and will require businesses to put a much stricter focus on data protection. The headline items for organisations that collect or process EU citizen records are:

- They must notify their supervisory authority of a data breach within 72 hours.
- The subject will have the right to retract consent, request data erasure or portability.
- They may face fines of up to 4% of their worldwide turnover, or €20 million for intentional or negligent violations.

These increased sanctions mean it is vital that the final legislative text be fully understood by a number of key stakeholders within the business, and that businesses start planning ahead as soon as possible.

To help them with that here are five key steps to help organisations perform a basic assessment of their current data protection strategy and any potential gaps that need filling.

Underpinning all of this is the fact, no matter how big a company is, that businesses have to begin thinking about their security in terms of when they will face an attempted data breach, rather than if. Only when businesses accept this will they be able to plan and execute successful security defences and policies.

By Neil Thacker, Information Security & Strategy Officer EMEA at Forcepoint

1

Identity

The first task for any organisation must be to identify whether they are considered a data controller or processor. They must then review the relevant obligations these carry, (such as issuing notices and obtaining consent), and regularly review existing and new processes around PII. They can then discover where this data resides – whether it is at-rest, in-motion and/or in-use – have a record of processing activities and understand how this data is protected.

2

Protect

Once PII has been identified it must then be protected. Encryption and access control are common control standards, but managing encrypted data across multiple business processes is a hugely difficult task. Data sovereignty and lifecycle are key, alongside data flows to third parties, monitoring for data leakage from negligent or malicious employees and external data theft.

3

Detect

If an organisation suffers data loss then it is vital to detect the breach and identify if PII records were lost or stolen. If so, the business must notify the authorities within 72 hours of the discovery to initiate a full investigation.

The investigation will focus on identifying the source and destination of the breach through information from Data Leakage Prevention (DLP) and Data Theft Prevention (DTP) tools. Data forensics will help to pinpoint the stolen data, so the business can issue notice to any affected data subjects.

4

Response

Incident response is critical to protecting EU citizen data. In addition to the mandatory data breach notification requirement, organisations must also ensure they have implemented and tested an effective incident response plan.

5

Recovery

In the aftermath of a data breach, businesses must ensure they maintain ongoing communication with the relevant authorities. This ensures secondary loss factors are managed and keep affected data subjects regularly informed.

TOP TIPS ON COMPLYING WITH THE EU GDPR

Jonathan Armstrong,
Founder and Partner of
Cordery Compliance

Announced in 2012, the long awaited European Union General Data Protection Regulation (EU GDPR) now looks set to come into force in spring 2018. In the current climate, where it seems we cannot go a week without a data breach or cyber-attack being reported (with December's JD Weatherspoon hack the biggest recent example), the new regulation can't come too soon.

European data protection laws haven't changed since 1995, when the Data Protection Directive was introduced. This seems like a lifetime ago when you consider how the data landscape has changed. For example, twenty years ago only one per cent of Europeans used the Internet, and in the past two years we have created more data than the past 2,000 years. The EU GDPR has been designed with this in mind, and represents more than just a fine-tuning of the existing regulation.

When it comes into force, the EU GDPR will have much stricter requirements for reporting data breaches and safeguarding customer data than current legislation, as well as more severe penalties. For example, everyone affected by a breach will need to be told if their information has been compromised, authorities must be notified of a breach within 72 hours, and companies over a certain size will need to appoint a data protection officer. Not only have the rules changed, but also the punishment – there will be increased sanctions for data breaches, including fines of up to 4% of an organisation's global turnover and potential criminal charges for executives.

Despite this, far too many organisations have not yet begun to think about the impact of the EU GDPR on their approach to data protection. With the stakes so high, businesses cannot afford to be complacent about complying with the EU GDPR. The sooner businesses are able to prepare and ensure they're compliant with the upcoming regulation, the better their chances of not falling foul of the Regulation when it comes into force.

With this in mind, we've compiled some essential top tips, outlining the actions that businesses must undertake now to ensure compliance.

1. **Understand the impact:** Put in place a data protection impact assessment policy so you understand how your business will have to adapt to the new regulation, and the potential impact of a breach.
2. **Thoroughly review vendor contracts**: Vendors' help will be needed to ensure compliance, especially in reporting security breaches. Organisations should make sure they have the contractual rights to insist on this and they should make sure that they can hold their vendors to account in the event of them causing a data breach.
3. **Recruit new team members**: Businesses over a certain size must recruit a Data Protection Officer, with smaller companies appointing someone responsible for data-related matters.
4. **Update everything:** Ensure new detailed documentation and records are ready for production for regulatory inspection - factor this into overhead costs.
5. **Day to day implementation**: Review how all of the key practical aspects of the EU GDPR, such as data retention and destruction, applies to all means of collecting data used by your organisation. If there are any discrepancies, then you need to review that particular method of collecting data.
6. **Create processes**: Put in place a data breach notification procedure, covering detection and response capabilities. It is also worth considering purchasing data breach protection insurance.
7. **Demonstrate compliance**: Create compliance statements for annual business reports. Not only will this show the wider world that you're compliant, but it will also ensure a consistent focus on this throughout the year.
8. **Deliver effective training**: This has never been more important, given the EU GDPR will be completely new to many of your employees. It will be vital that your staff are thoroughly trained on all of the above.

There will be considerable challenges to comply with the new rules. The less time your organisation has to make sure all of its systems and processes comply with the new rules, the harder it will be. What's more, rushing through the changes needed will inevitably lead to errors, which could result in breaches and costly fines. However, a measured approach, using the time available, will allow you to successfully navigate the increasingly stormy seas of data regulation, and reach compliance before the EU GDPR hits with full force.

Contact us today at **www.securityplusonline.co.uk** to learn more about GDPR.

CYBER ESSENTIALS:

YOUR FIRST STEP IN CYBER SECURITY ACCREDITATION

By Ian Glover,
President of CREST

Both public sector and private sector organisations are beginning to realise that even if they have implemented effective cyber security controls, their suppliers may provide a weak link. So, if any organisation wants to prove to its clients that it takes security seriously, getting Cyber Essentials certification is a very good first step.

Cyber Essentials was launched in 2014 as part of the UK Government's National Cyber Security Strategy and introduces an entry-level cyber security standard that is achievable and affordable for any size of organisation across any type of business. It sets a baseline for cyber security and provides an independent assessment of the security controls that you need to have in place to mitigate risks from the most common forms of cyber threats.

Not only will your business be more secure, but displaying the Cyber Essentials 'badge' will demonstrate that you have taken steps to be cyber safe – giving you a distinct edge over your competitors. What's more, the **UK Government already mandates suppliers to be Cyber Essentials certified if they are bidding for contracts that involve handling sensitive and personal information**.

The scheme focuses on five cyber security controls to help to reduce your company's cyber risk. These are: boundary firewalls and internet gateways, secure configuration, access control, malware protection and patch management.

Cyber Essentials shows that an organisation has taken steps to be cyber secure but it is designed only to provide basic cyber hygiene.

The two levels of certification

The first stage in the certification process is to decide which level to certify against:

- **Cyber Essentials**: organisations complete a self-assessment questionnaire which is reviewed by an external Certifying Body.
- **Cyber Essentials Plus:** tests of an organisation's systems are carried out by an external Certifying Body.

Both include a questionnaire which relates to security controls and the secure configuration of an organisation's computing resources, and a remote technical assessment to validate elements of the questionnaire.

The key differentiator for Cyber Essentials Plus is the inclusion of a technical review of the organisation's workstations, increasing the validity of certification considerably by providing evidence of compliance against the following scenarios:

- Can malicious files enter the organisation from the Internet through either web traffic or email messages?
- Should malicious content enter, how effective are the anti-virus and malware protection mechanisms?
- Should the organisation's protection mechanisms fail, how likely is it that the organisation will be compromised due to failings in the patching of the organisation's workstations?

Cyber Essentials Plus is a more thorough assessment of the organisation and so may provide greater security assurance, but does come at an additional cost.

How to get certified

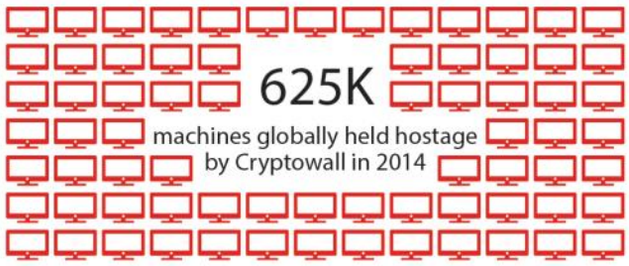
Once a decision has been reached to proceed with a Cyber Essentials certification, a Certifying Body must be appointed to carry out the assessment.

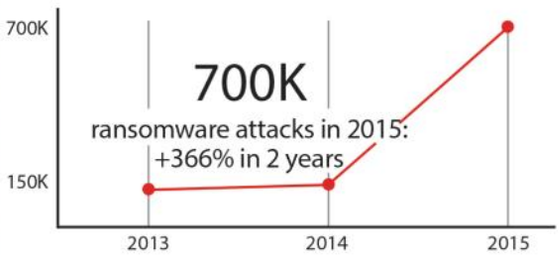
Organisations have a number of certified suppliers that they can select, all of whom have to be accredited by one of these four Government appointed organisations: CREST and IASME who contributed to the design and development of the scheme, along with APMG Group and QG Business Solutions. **You can find out more about Cyber Essentials and how to select a company to help you on the Cyber Streetwise web site: at www.cyberstreetwise.com/cyberessentials/**

Once an organisation has been assessed against the Cyber Essentials security criteria and passes, they will receive the relevant Cyber Essentials award (badge) based on the level of certification achieved. It is important to remember that Cyber Essentials is not a silver bullet and must instead be seen as a basic good start to becoming more secure. If an organisation is part of the supply chain, they must also understand their obligations and not become the weakest link in the chain and therefore the most logical to attack.

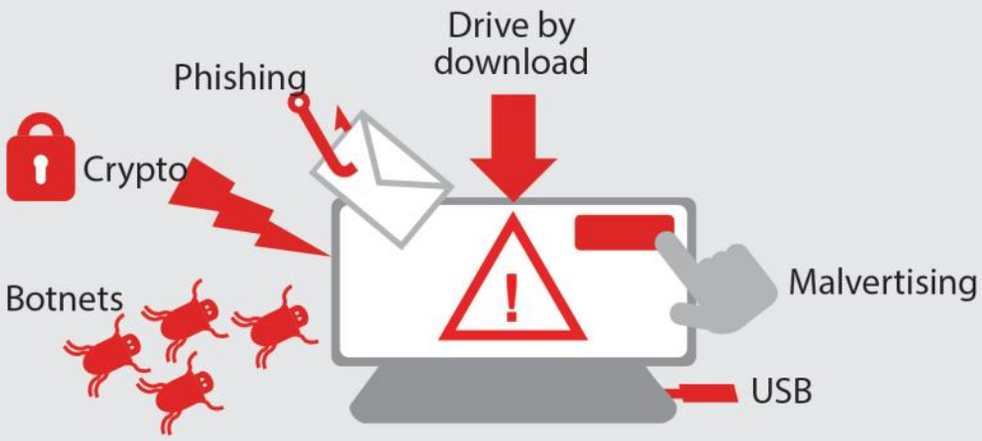
Ian Glover is president of CREST, the not for profit accreditation body for the technical information security industry.

Why you should care about ransomware

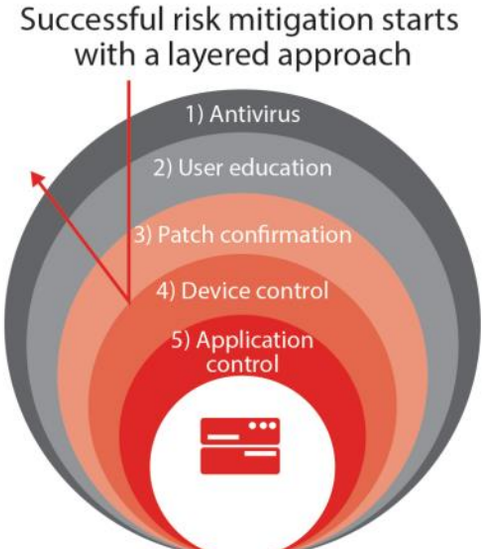




How it attacks the network



Defence in depth: avoiding extortion



Provided by HEAT software

HIT BY RANSOMWARE?
HOW TO ENSURE BUSINESS CONTINUITY

One of the biggest trends of 2016 is the rise of ransomware— malware that brings a very distinct headache for many who suddenly find themselves in need of an effective data recovery tool. Ransomware takes a number of approaches, from attempting to trick computer users into believing a local police authority has detected illegal software on their computer and that they must pay a fine in order to regain access to the data, to simple extortion by demanding a Bitcoin payment to unlock data the malware has encrypted. With victims from home users to corporations, it seems no one is safe.

Police Department pays ransom to regain data access

One recent high profile case was in Swansea, Massachusetts (USA), where the local police department gave up $750 to regain access to their computers. This particular version was named CryptoLocker, which found its way into the police department's system when an unsuspecting employee opened a malicious email attachment.

Given the good-old-fashioned advice to never open an email attachment from an untrusted source, one might speculate the user was ill-trained. But these emails can be deceiving, claiming to be from government agencies like the FBI, including official agency logos and disguising the malware as a PDF attachment. Once the attachment was opened, CryptoLocker encrypted all the files on the computer, requiring the victim to pay a fee in exchange for the access code.

All cybercrime roads lead to enterprise

The biggest problem in dealing with threats like Ransomware is poor preparation. While prevention is without doubt better than cure, malware can find a way in—and organisations can't recover their data if they don't have a strong backup recovery tool in place. Just backing up data to a mapped network or hard drive or even creating regular backup images won't help if the backup isn't secure. Ransomware will encrypt all the data on a PC, including all connected drives, which means your backups become useless.

Companies can even lose access to the data on network drives or even the entire enterprise network. Ransomware such as CryptoLocker encrypts any data it finds on any mapped drive, even if the data on that drive is in the cloud. We can expect this software to attack any connected network in the near future, since a code change to make that possible would be almost painfully easy.

Wired.com's Patrick Oliver Graf put it so well: "*Even more worrisome is that beyond individual files, the network itself could be held for ransom, if a hacker gained the necessary read and write privileges by infiltrating a network administrator's device. Cybercrime goes where the money is, and eventually, all roads lead to the enterprise.*"

Creating an effective defence and recovery policy is not simple. It needs to include a number of layers—including:

- Robust endpoint protection,
- Email security to prevent malicious emails that often initiate the attack
- Application control, that can be an effective defence stopping malware executing in the first place.

To be fully protected, companies need a combination of several strategies and that should include an effective recovery tool to be used as a safety net should the security measures fail.

A business continuity solution that incorporates backup and recovery can secure vital data where it can be accessed from strategically placed servers in the event of a catastrophic data failure. Less vital data can be stored on tape to be retrieved and restored once the system is up and running again.

In the case of a ransomware attack, enterprises must think about the infected network as well. Disconnect all infected computers from all network communications so your tech staff can clean them before putting them back into service. A company can be up and running faster by keeping backup machines available that remain offline when not in use. These systems can be brought from storage and used to keep the business running while technicians clean infected computers of the virus.

Contact us to learn how to provide essential business continuity to protect against productivity loss from malware.

Quorum®

Learn more about Quorum and request your demo at www.securityplusonline.co.uk/quorum