RANSOMWARE ATTACKS RISE

AVOID BEING THE NEXT VICTIM OF CYBER CRIME AND REDUCE THE THREATS AGAINST YOUR ORGANIZATION

OVERVIEW

The past year has been a busy one for cyber criminals, with over 500 data breaches and more than 500 million records exposed in 2015. This includes the disclosure of 21 million U.S. Office of Personnel Management (OPM) records, the 70 million medical records at Anthem and the 37 million user details at infidelity site Ashley Madison. The health, retail, technology, financial and governmental sectors head the list of business areas that were the most targeted throughout the year.

“Ransomware” is on the rise using “targeted phishing attacks” and are being used for financial blackmail and to gain access to confidential information and poison or corrupt data. No one is excluded from these threats and no company or individual is too small to be a target.

Ransomware has become such a major threat due to its many variations and its drastic impact in restricting access to systems and data therefore making day to day business unavailable and shutting down access to critical systems.

Existing perimeter solutions today have failed to detect and prevent Ransomware from infecting and spreading within the organizations networks creating mass operational disruption and with signature based anti-virus unable to prevent and detect due to the uniqueness and quickly growing variants of ransomware.

The US CERT and DHS Threat Alert explains the nature of the threat very well and outlines several solutions available. The FBI also recently added a list of recommendations similar to those below.

US-CERT recommends that users and administrators take the following preventive measures to protect their computer networks from ransomware infection:

- **Employ a data backup and recovery plan for all critical information.** Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
• **Use application whitelisting to help prevent malicious software and unapproved programs from running.** Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.

• **Keep your operating system and software up-to-date with the latest patches.** Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.

• **Maintain up-to-date anti-virus software, and scan all software downloaded from the internet prior to executing.**

• **Restrict users’ ability (permissions) to install and run unwanted software applications, and apply the principle of “Least Privilege” to all systems and services.** Restricting these privileges may prevent malware from running or limit its capability to spread through the network.

• **Avoid enabling macros from email attachments.** If a user opens the attachment and enables macros, embedded code will execute the malware on the machine. For enterprises or organizations, it may be best to block email messages with attachments from suspicious sources. For information on safely handling email attachments, see Recognizing and Avoiding Email Scams. Follow safe practices when browsing the Web. See Good Security Habits and Safeguarding Your Data for additional details.

• **Do not follow unsolicited Web links in emails.** Refer to the US-CERT Security Tip on Avoiding Social Engineering and Phishing Attacks for more information.

In 2016 we are now seeing an evolution of targeted attacks against organizations where Ransomware is being used for criminal activity against time sensitive data. These types of threats are expected to rise significantly in the future and it is important that organizations act now to reduce the risk of loss of data and more importantly the loss of critical infrastructure like energy, water, emergency services and transportation.

Credit Card and Identity theft is a very profitable business for cyber criminals though critical infrastructure has a different type of value where it relates to not financial risk but the risk of the lives of the people they are associated with and turns decision making into a high risk for those making life threatening decisions based on the veracity of the data available in a time sensitive window.

Many systems pose quite an easy target for attackers since they are typically running legacy operating systems, security updates are less applied in the concern of breaking the systems, security compliance and complexity of the systems make security a larger task and therefore typically has been lower in priority.

Many companies are still vulnerable and will continue to be vulnerable to cyber attacks and data disclosures until they implement more secure measure to protect, detect and respond against these threats.
WHAT ADDITIONAL STEPS CAN BE TAKEN?

UNDERSTANDING HOW THE HACKERS OPERATE WILL GIVE YOU CYBER ADVANTAGE

In an advanced threat, the attacker will spend a large amount of time researching a list of potential targets, gathering information about the organization’s structure, clients etc. Social media activity of the people in the target company will be monitored to extract information about the systems and forums favored by the user and any technology vulnerabilities assessed. Once a weakness is found the next step the attacker will take is to breach the cyber security perimeter - the basic security most companies adopt - and gain access, which, for most attackers, is easily done.

ONCE CYBER PERIMETERS ARE BREACHED HACKERS CAN MOVE AROUND UNDETECTED

Once inside an organization’s systems, the attacker maps the network in order to gain access to higher value assets and to elevate privilege access rights so he/she can move more freely around the company undetected. The importance of network segmentation and threat detection is vital to prevent the ease of pivot building and lateral moves across the network. By compromising a single system should not mean that an attacker has privileged access that can be used to easily move around the network, the importance of privileged account management solutions can help make lateral moves more difficult for an attacker and also be a detection indicator for a immediate threat.

Therefore local and shared account password randomization and management can prevent and limit these techniques used making the task of an attacker more difficult. This can also be used in the scenario when a breach is detected in one department or systems you can then use this as a break the glass in order to quickly lock down other systems and endpoints from being impacted by the active breach, this type of scenario locks down the accounts and increases the protection on each system.

THE BIGGEST RISK OF THE EMPLOYEE USING IT SYSTEMS AND RESOURCES IS THE PRIVILEGED ACCESS THEY HAVE

The biggest risk is from employees using IT systems since security prevention mechanisms within the network itself are rarely implemented in the mistaken belief that perimeter defenses are all that is required.

This, however, is where most companies need to invest more; to detect when these types of activities are occurring and reduce the breach “dwell time”. This is the period, currently averaging 205 days, before an attack is detected; a time in which the attacker has gained access, avoided detection, taken information and left without a trace. By moving to least privilege will mean that the employee will only have access to the resources and applications they require to do their work and therefore do not have elevated privileges that could result in a cyber catastrophe.
LEAST PRIVILEGE AND APPLICATION WHITELISTING

Do not allow users to install or execute unapproved or untrusted applications

Stop Malware and Ransomware at the endpoint

Another major risk that organizations have resulting from providing users with privileged access is that the user has the ability to install and execute applications as they decide no matter where or how they obtained the installation executable. This can pose a major risk allowing Ransomware or malware to infect and propagate into the organization as well as allow the attacker to install tools, which allows the attacker to easily return whenever they wish. If a user with a privileged account is simply reading emails opening documents, browsing the Internet and clicking on numerous links or they simply plug a USB device into the system this can quickly install infectious or malicious tools that allow an attacker to quickly gain access and begin the attack from within the perimeter or in a worse case scenario encrypt the system and sensitive data requesting for a financial payment in return to unlock them.

Organizations should implement security controls that prevent any application or tool from simply being installed onto the system by using Application Whitelisting, Blacklisting, Dynamic Listing, Real-Time Privilege Elevation, and Application Reputation and Intelligence. This is one of the most effective ways to prevent being the next victim of cyber crime.

PATCH MANAGEMENT CAN MITIGATE MORE THAN 80% OF CYBER ATTACKS

Another major concern is the ever growing and increasing complexity of patching systems and applications. This is typically more complicated in the retail industry due to distribution, remote access and limited bandwidth available as well as poorly trained end-users operating these technologies.

The importance of “patch management” is huge since it can mitigate more than 80% of cyber threats, leaving only those nasty zero days to deal with. Vulnerabilities are growing each year and out of the exploited vulnerabilities in 2014, 99.9% of them had a CVE (Common Vulnerabilities and Exposures) published.

DON’T GIVE EMPLOYEES LOCAL ADMINISTRATOR ACCOUNTS OR PRIVILEGED ACCESS

Passwords and privileged accounts should be a major concern for many organizations. These can be the difference between a simple perimeter breach and a cyber catastrophe.

Companies should provide suitable training for employees on best practices for password choices, normally a very complex password is required though many employees revert to writing them down due to difficulty in remembering them or use the same password for corporate and personal social accounts. This leads to a possible external threat, which companies should continuously assess.

If your company is giving employees local administrator accounts or privileged access then this seriously weakens the organization’s cyber security. This can mean the difference between a single system and user account being compromised and the entire organization’s computer systems. In all Advanced Persistent Threats the use of privileged accounts has been the difference between a simple perimeter breach and a major data loss, malicious activity, financial fraud occurring or worst case Ransomware.

Organizations should quickly ensure that they continuously audit and discover privileged accounts and applications that require privileged access, remove administrator rights where they are not required and adopt two-factor authentication to mitigate user accounts from easily being compromised.
PERFORM CONTINUOUS CYBER SECURITY ASSESSMENTS

Performing continuous cyber security assessments is another key factor in mitigating risks. While these assessments are often considered as a “checkbox” means of passing or complying with regulations, they should be approached as a method to evaluate the state of cyber security. They can be used also to evaluate incident response capabilities, detect if an active breach is in progress, and to keep the company security conscious.

GOT TECHIE USERS IN YOUR OFFICE? GET THEM CYBER SECURITY AWARENESS TRAINED

Cyber security awareness training should be at the top of the agenda.

This is one of the most effective ways of reducing a company’s exposure to cyber security threats and increases both detection and incident response at the same time.

It is highly recommend that training start at the top of the organization, working down. It is also recommend that a company appoint a cyber/security ambassador within each department to assist in the detection and incident response for potential cyber security threats and risks. This helps expand the efficiency of any IT security team, while ensuring that there is someone in the organization who is responsible and accountable for implementing and maintaining cyber security measures.

BE DECEPTIVE, BE UNPREDICTABLE

A very important recommendation is to be deceptive, be unpredictable. Most organizations look to automation to help assist in their cyber security defenses but in many this lends itself to predictability: scans are run at the same time every week, patches take place once per month, assessments once per quarter or per year.

Companies that are predictable are very vulnerable, so should establish a mind-set in which systems are updated and assessed on an adhoc basis. Randomize your activity. This will increase your capability in detecting active cyber attacks and breaches.