XM CYBER®

TOP 10 TIPS TO SPRING CLEAN YOUR CYBER SECURITY

By Amit Waisel, Senior Technology Lead in Security Research, XM Cyber

With spring in full swing, organizations should dedicate time to scrubbing and sprucing up their security.

For many households, clearing clutter is an annual ritual that marks the end of winter and the beginning of spring. For organizations, a digital spring cleaning is key for avoiding data breaches.

More than 4.5 billion records were compromised in the first quarter of 2019, reported IT Governance. Last year, the global average cost of a data breach was $3.86 million and the average cost for each lost or stolen record containing sensitive and confidential information was $148, according to a Ponemon Institute study.

While many CISOs still consider zero-day threats one of their chief concerns, they are being employed much less frequently. Most cyberattacks are surprisingly unsophisticated – so simple, in fact, that the NSA reports 93% of them could be prevented just by incorporating some basic best practices.

It's important to highlight that hackers no longer need to put in the time-consuming effort necessary to create elaborate new attacks, because they know they can sneak through companies' defenses just by taking advantage of poor IT hygiene.

This is the very reason for this article. To kick off the new season, XM Cyber has pulled together a few smart steps to improve your IT hygiene and reduce the risks of your company joining the year's dreaded list of breach victims.

POLISH YOUR PASSWORD MANAGEMENT

Using a different password for each of your online accounts seems tough for most people. After all, remembering them all can be nearly impossible, particularly if you want to use strong logins that are difficult to crack. The solution to these problems is a secure password manager, which will generate strong passwords using a combination of letters, numbers and special characters and store them in an encrypted vault. My tip: Cloud-based password managers can get hacked. That's right -- any online-based solution may itself be a target. Use an offline password manager with multi-layer encryption, like a private key, together with a strong but unique password you can remember.

ELIMINATE LOGIN RISK WITH MULTI-FACTOR AUTHENTICATION

Using multi-factor authentication is currently the best way to add an extra layer of security to your online accounts for services like Google, Facebook, Twitter, Dropbox, and many others. Usually, it involves sending a unique code sent to your smartphone that you enter along with your password. Or you can generate an individual code, using mobile apps like Google Authenticator or Microsoft's Authenticator app. It can also be done using something you have, like a special USB key with a unique token or biometric data from an iris scan or fingerprint. It's important to say multi-factor authentication is relevant only during the login phase. It doesn't help protect your device in other attack phases.

SWEEP OUT UNATHORIZED APPLICATIONS

Apply application whitelisting in your organization and only authorized software will be allowed to run. This way, unknown executable files, malware or ransomware cannot run. Whitelisting is a very good practice that I strongly recommend to most IT administrators to prevent unauthorized executable files or programs from running on their system. Home users, too, can take advantage of whitelisting.

CLEAR OUT EMPLOYEES' DOUBTS BY EDUCATING THEM

One of the biggest vulnerabilities in organizations' IT is their people. Protecting your systems from online threats starts with educating your employees -- it's the best way to prevent high-profile breaches. Ironically, one aspect of IT security that is often overlooked is the easiest – and usually cheapest – to implement: employee education. Training and educating your employees, no matter the size of your business, should be one of your top priorities. That may include internal campaigns against phishing attacks (e.g. sending reminders about suspicious links and attachments) and several other topics. Be creative and communicative.

Email is one of the main delivery vehicles for phishing attacks, along with malware campaigns such as ransomware attacks. Bad actors are using increasingly complex psychological techniques to send credible emails, getting even the most trained and sophisticated users to click on links and attachments. Phishing simulator tools monitor millions of emails, URLs, files, and other data points each day for the latest threats. To protect your assets, give your employees supplementary training. Help them understand how to spot an advanced attack and prevent future breaches.

ELIMINATE ADMIN PRIVILEGE TO USERS WHO DON'T NEED THEM

This means you must revoke the rights of employees who don't need them. When more people have access to company data but are not knowledgeable about information security, this means a higher risk of data and security breaches for your business. Limit the number of users with administrative privileges. The rule is simple: Don't be generous, ask the real need for the user's everyday work. Don't give security shortcuts.

ELIMINATE JOINT WI-FI CONNECTIONS FOR EMPLOYEES AND GUESTS

Companies should provide a guest Wi-Fi network that is separate from their private network infrastructure. Hackers can penetrate a victim's computer without their knowledge and then pivot to other information systems. Ensuring that only computers and devices approved by a company's information security personnel have access to the private network will make it more difficult for attackers to penetrate that barrier.

CLEANSE (OR AT LEAST LIMIT) BYOD

While a large majority of companies now permit employees to use their own devices for work, they have concerns over security and privacy. What's scarier is that some organizations are extending the BYOD (bring your own device) practice to contractors, partners, customers, and even suppliers. Security concerns are the main barrier to BYOD. The main worry is data leakage, followed by unauthorized access to data and an inability to control uploads and downloads.

CLEAN OUT PUBLIC CONNECTION RISKS WITH VPN

Many employees work remotely through network access points or “hotspots” that are outside of the company’s IT team’s control. Yet bad actors can spoof what may look like legitimate hotspots to lure victims to send traffic (such as emails, passwords and documents) through their equipment, thereby stealing data. Mitigate this risk by offering users a virtual private network (VPN) that provides end-to-end encryption for the data the employee is transmitting so that it is much more difficult for the adversary to exploit the data.

CLEAR EXPOSED SENSITIVE DATA BY ENABLING FULL-DISK ENCRYPTION

Ensure your organization’s computers have full disk encryption enabled. This will protect information by converting it into unreadable junk that cannot be deciphered easily by unauthorized people. Full disk encryption has several benefits compared to regular file or folder encryption, or encrypted vaults. Nearly everything, including the swap space and the temporary files, is encrypted. With full disk encryption, the decision of which individual files to encrypt is not left up to users’ discretion.

SHINE YOUR CROWN JEWELS WITH AN AUTOMATED PURPLE TEAM

Simulate, validate and remediate attack paths to your critical assets with a fully automated breach and attack simulation (BAS) platform. XM Cyber’s HaXM continuously exposes attack vectors, above and below the surface, from breach point to any organizational critical asset. This continuous loop of automated red teaming is completed by ongoing and prioritized actionable remediation of organizations’ security gaps. In effect, HaXM by XM Cyber operates as an automated purple team that fluidly combines red team and blue team processes to ensure that organizations are always one step ahead of the cyber-attackers.

ABOUT XM CYBER

XM Cyber was founded by security executives from the elite Israeli intelligence sector.

XM Cyber’s core team is comprised of highly skilled and experienced veterans from the Israeli Intelligence with expertise in both offensive and defensive cyber security.

XM Cyber has developed more than 15 patented technologies based on a proprietary set of algorithms that enable the continuous and automatic simulation of a hacker’s techniques and methods.

AMIT WAISEL

Amit Waisel is a Senior Technology lead in Security Research at XM Cyber. He is a seasoned data security expert with vast experience in cyber offensive projects. Prior to XM Cyber, Waisel filled multiple data security positions in the Israeli intelligence community. Waisel is well experienced with malware detection and analysis techniques, operating system internals and security-oriented software development.