Getting Back to Basics
Protecting Organizational Assets and Confidential Information

If you are like me, and receive daily digests and alerts of the latest news on the IT Security front, it seems that lately, we are being bombarded by news of increased threats be they Hacktivism (state sponsored or other), denial of service (DDOS) attacks against well known institutions, advanced persistent threats (APT), ransomware (also referred to as cryptoviruses, cryptotrojans, cryptoworms or scareware), malware, Data Loss Protection (DLP) and more, I sometimes want to advise my clients to simply disconnect from the internet to protect themselves.

This in addition to the copious amounts of 'whitepaper's', that impart individuals with fear that unless they purchase a specific product they will be at risk of threat, intrusion, and more.

I wonder what goes through the Director of IT's mind – how do I protect my organization with limited budget when attacks seem to be coming from everywhere. Should I – rip and replace with new technologies, focus on BYOD, lock down the network to the detriment of workflow and productivity, disallow all social networking – Twitter, Facebook or all of the above.

While I am not about to say there is nothing to worry about - the threats are real and in some cases extremely hazardous to an organizations network and reputation, but it is time to get back to the basics.

While it is clear that the threats that we face today are more complex than they were 5 years ago, it is also making it more difficult to define what needs to be protected. In addition to dealing with the plethora of new technologies which have redefined the way we work to address these threats, regulatory restrictions and guidelines have introduced an additional complexity into the mix.

Key concepts which were defined years ago still provide the best guidelines to start.

Numerous organizations provide guidelines on security for organizations – SANS (SysAdmin, Audit, Network, Security) which was established in 1989, and the National Institute of Standards and Technology (NIST) is where most organizations should refer to for assistance.

One of the most comprehensive reports on protecting your network – Critical Controls for Effective Cyber Defense, published by SANS (*www.sans.org/critical-security-controls*) – is a great starting point. This document provides for 20 critical controls and it begins by stating take an inventory of your authorized and unauthorized devices, then take an inventory of the authorized and unauthorized software in use at your organization. In my job it amazes me that when I speak to a person who is looking for security software and when I ask a simple question such as how many devices do you

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477
www.symtrex.com
sales@symtrex.com

symtrex inc.
Network Security Specialists

have in your network, I get vague responses, as opposed to a defined answers. The truth of the matter is that you cannot protect what you don't know you have, or have control of. There are tools out there that can provide you with the answer to this, they are cost effective and can provide a wealth of information at your finger tips.

Once you have your Security Posture Assessment (SPA), then you can work at providing for a secure configuration for your hardware and software. This includes all hardware – mobile, servers, workstations, etc and the associated software on each.

The next step is to define your network; you need to know your assets and what needs to be protected. Here is where things get a bit more involved. Almost all organizations have a firewall, as well they permit users to connect to the internet, receive email, and may have permitted for wireless access for both employees and guests. Will a firewall stop all malicious intent? Unfortunately no. Firewalls by their very nature allow communication through open ports, and in the past malicious attempts were made against the firewall, the bad guys got smart and said to themselves, why break down the wall when I can knock and someone will let me in! Threats now come in a myriad of forms, and can enter the organization via browsing the web (Java exploits) , emails (Phishing, Spear Phishing, Clone Phishing, Whaling) and mobile/wireless. The use of some form of Endpoint Security (each computing device on a corporate network to comply with certain standards before network access is granted) should be considered, and specifically endpoint software where you can push out updates so that everyone is at the latest update or standard is better. Some Endpoint solutions also provide for application monitoring as well as encryption, so again, once you know what you need to protect you can make a knowledgeable decision.

If you have a website (and again almost all organizations have one), and you host it, if it is a dynamic website built using a Content Management Sysytem (CMS) or customized software, you need to ensure that the site is protected. CMS Systems can be easily comprised using Cross-site scripting (XSS) where the attackers inject client side scripts into Web pages on your site. This is another way that those with malicious intent can harm your organization and your organizations reputation.

One area that I will mention only in passing, however it is by no means low on the list is restrict software installation, updates, etc to those with administrative privileges. This is to prevent Drive-By installation (Any download that happens without a person's knowledge) of malicious software. This does not mean providing end users with those privileges, but rather that a set procedure is put in place, and only those with administrative privileges have the authority to install software. Now, what about a device that connects that is not owned by the organization but rather it is the employees. There is growing debate surrounding the discussion on if an organization should be allowed to install software on a mobile device that the corporation or organization does not "own" but is employee owned (BYOD). The real question is how much risk you want to take. If an

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477
www.symtrex.com
sales@symtrex.com

symtrex inc.
Network Security Specialists

employee uses his laptop or mobile device to connect to the network, then it would be best practices to at least ensure that his device is clear of malware, viruses or similar.

In addition, a Vulnerability Assessment (VA) of your network should be done on a regular basis, as we are all human, and having another set of eyes confirming the status of your network is always a good idea. Vulnerability assessments ensure that the perimeter is protected using tools that most hackers have access to, as well it confirms your Security Posture Assessment (SPA). If remediation can be done in a timely fashion, it can provide you with piece of mind.

Again looking at the perimeter - or more specifically the end points. One of the biggest threats to an organization is the employees, and human nature. While it is great to provide training, as well as provide a "best practice" or "Corporate Policy" document, these do not eliminate human error, such as releasing an email from quarantine that they believe might be legitimate or similar, which then launches malware or APT's through the network. It still amazes me that users can be fooled by the UPS package delivery emails at Christmas, or phone calls from someone from Microsoft telling them that they have a virus (Social Engineering). While technology has been around for what seems like an eternity, and most of us do not have any idea how we were able to function before the time of instant access to information, emails, electronic funds transfer, technology is still a mystery to some, and they need to be advised how to use it effectively and securely.

Once this is all done, remember to monitor and review your log files from all devices, applications, etc. Not only do logs provide invaluable information for your team but regulatory acts and compliance guidelines require you to review your log files. If monitored on a regular basis they can provide you with information on unusual activity, suspected access, failed logons, etc as well as provide system information to your support team. Logs are the glue that holds everything together.

The last point, after you have this all setup, do not think that you are done. In order to safely, effectively and efficiently protect your assets and proprietary information, these reviews have to be done on a continual basis. There is not a single product or company that can say, "if you use my product your network will be safe". Ultimately it is up to the organization to continually work on this, and it is up to the IT staff to be able to say that using our current technologies, as well as following simple yet effective steps they can be confident that you are as protected to the best of their ability. It is also a best practise to schedule Vulnerability Assessments or Penetration Testing (even if not required by a compliance regulation) just to make sure that no items were missed and current exploits are remediated.

I do highly recommend that you download the SANS Critical Control for Effective Cyber Defense. If you have any questions or would like some additional information, please contact us at 866-431-8972 or www.symtrex.com

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477
www.symtrex.com
sales@symtrex.com

symtrex inc.
Network Security Specialists