15 ways to improve your cyber security WITHOUT SPENDING A CENT

Implementing everyday security initiatives to protect your environment

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

THE COST OF SECURITY

Experts predict that worldwide, cybercrimes of all kinds will cause losses of $6 trillion annually by 2021.[1] The biggest cyber security threats to the middle market currently include ransomware, social engineering, business email compromise and data loss from advanced persistent threats.

We all know from experience that cyber security is constantly changing. Although security cannot be bought per se, most security systems and initiatives do have associated costs—and must be budgeted for and funded. However, the following 15 recommendations outlined in this e-book do not have any associated costs at all.

15 STEPS YOU CAN TAKE TODAY

1 | DISABLE LOCAL LINK MULTICAST NAME RESOLUTION

2 | DISABLE NETWORK BASIC INPUT/OUTPUT SYSTEM (NETBIOS) NAME SERVICES

3 | DISABLE WEB PROXY AUTO-DISCOVERY **4** | CHANGE DEFAULT CREDENTIALS

5 | REMOVE LOCAL ADMIN RIGHTS **6** | SET UNIQUE LOCAL ADMIN PASSWORDS

7 | UPDATE POWERSHELL **8** | HARDEN YOUR HOSTS **9** | PROTECT YOUR STORAGE

10 | ADOPT A LEAST PERMISSIONS APPROACH **11** | VERIFY BACKUP INTEGRITY

12 | AGGRESSIVELY PATCH EVERYTHING **13** | EDUCATE YOUR USERS

14 | USE DATA-AT-REST ENCRYPTION **15** | TAG EXTERNAL AND SUSPECT EMAIL MESSAGES

[1] "Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021," PR Newswire, accessed Feb. 11, 2019, https://www.prnewswire.com/news-releases/cyberattacks-are-the-fastest-growing-crime-and-predicted-to-cost-the-world-6-trillion-annually-by-2021-300765090.html.

1 | DISABLE LOCAL LINK MULTICAST NAME RESOLUTION

Local link multicast name resolution (LLMNR) is a noncritical Windows service that is often abused by hackers to gain credentials that can further an attack. Usually enabled by default, LLMNR is a peer-to-peer domain name service (DNS) protocol that sends out multicast messages requesting addresses for network resources.

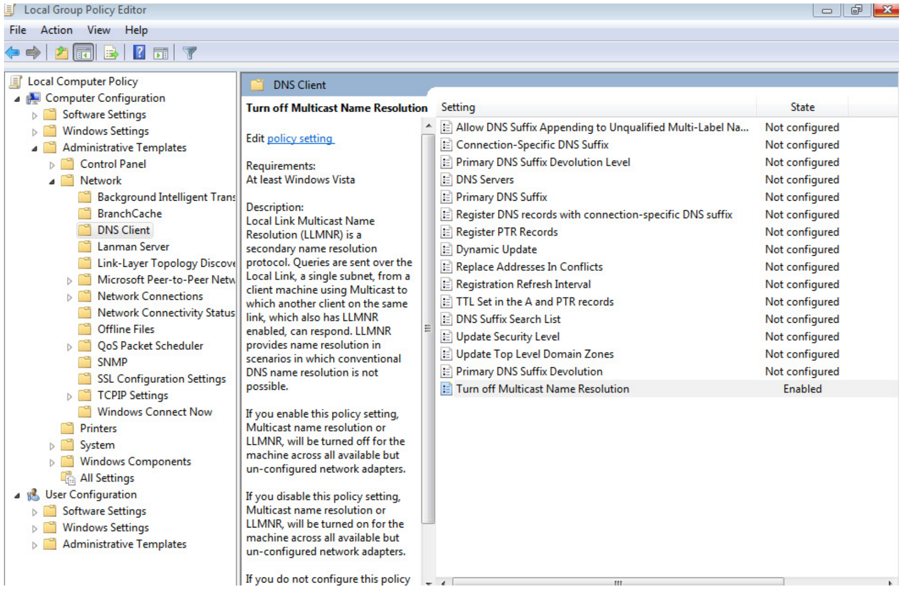
Simply put, LLMNR is a name resolution service that helps one system look for another system or something else specific on the network. The service will go out and try to figure out how to resolve the name and how to get an address for it. This can be exploited because the service, by nature, assumes that anything that is responding to it on the network can be trusted.

Attackers use readily available hacking tools found on the internet to send a fake response back and cause a user's workstation to send credential information to their fake machine. It will then capture credentials in the form of a hash and the attacker can then use that hash in multiple ways—pass the hash where they use it to authenticate and use against other systems or technologies with the user's credentials or they can crack that hash and end up getting the user's exact username and password.

LLMNR employs no security or authentication components and is simply a Microsoft networking feature that helps make networking easier. Many people don't even know what LLMNR is and honestly most Microsoft networks do not need it.

However, turning this feature off is very simple. In order to disable LLMNR, create a group policy object (GPO) within your active directory structure. Next, set a computer configuration to turn off multicast name resolution. This can all be done without spending any money—it just takes a little time to create a GPO, test it and deploy to all Windows systems.

As a visual guide, here's what it will look like from a GPO perspective. If you are setting the group policy, a setting says, "turn off LLMNR." By enabling it or essentially turning it off, there will be one less problem to worry about on your network.



Turn off Multicast Name Resolution

Edit policy setting

Requirements:
At least Windows Vista

Description:
Local Link Multicast Name Resolution (LLMNR) is a secondary name resolution protocol. Queries are sent over the Local Link, a single subnet, from a client machine using Multicast to which another client on the same link, which also has LLMNR enabled, can respond. LLMNR provides name resolution in scenarios in which conventional DNS name resolution is not possible.

If you enable this policy setting, Multicast name resolution or LLMNR, will be turned off for the machine across all available but un-configured network adapters.

If you disable this policy setting, Multicast name resolution or LLMNR, will be turned on for the machine across all available but un-configured network adapters.

If you do not configure this policy

Setting	State
Allow DNS Suffix Appending to Unqualified Multi-Label Na...	Not configured
Connection-Specific DNS Suffix	Not configured
Primary DNS Suffix Devolution Level	Not configured
DNS Servers	Not configured
Primary DNS Suffix	Not configured
Register DNS records with connection-specific DNS suffix	Not configured
Register PTR Records	Not configured
Dynamic Update	Not configured
Replace Addresses In Conflicts	Not configured
Registration Refresh Interval	Not configured
TTL Set in the A and PTR records	Not configured
DNS Suffix Search List	Not configured
Update Security Level	Not configured
Update Top Level Domain Zones	Not configured
Primary DNS Suffix Devolution	Not configured
Turn off Multicast Name Resolution	Enabled

2 | DISABLE NETWORK BASIC INPUT/OUTPUT SYSTEM (NETBIOS) NAME SERVICES

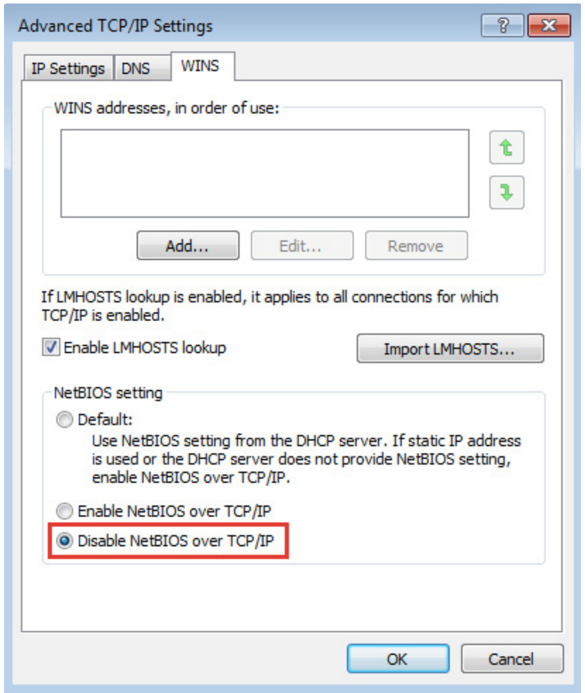
Like LLMNR, NetBIOS name services (NBT-NS) is a noncritical Windows service that hackers can infiltrate to gain credentials and launch an attack. NBT-NS is also a peer-to-peer DNS protocol that sends out multicast messages requesting addresses for network resources.

NBT-NS is limited to networks using IPv4, which is most networks, and is typically enabled by default. Without security or authentication components, NBT-NS is also a Microsoft networking feature created to make networking easier, but most networks do not have a use for it. This feature can also be exploited by some of the tools readily available on the internet such as Metasploit that can take advantage of the NetBIOS name service.

To easily disable NBT-NS, set an option in the dynamic host configuration protocol (DHCP) scope or manually disable it on systems with statically-assigned IP addresses. The fix will then get pushed out whenever the IP address receives a DHCP request. It's also possible to disable by GPO by setting the NetBIOS node type to P-node.

Again, this can all be done at no cost by simply updating the DHCP scope settings and manually disabling NetBIOS over TCP/IP on systems that do not use DHCP.

The following screen shots show how disabling the NBT-NS will look through DHCP.



Advanced TCP/IP Settings

IP Settings | DNS | WINS

WINS addresses, in order of use:

Add... Edit... Remove

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

Import LMHOSTS...

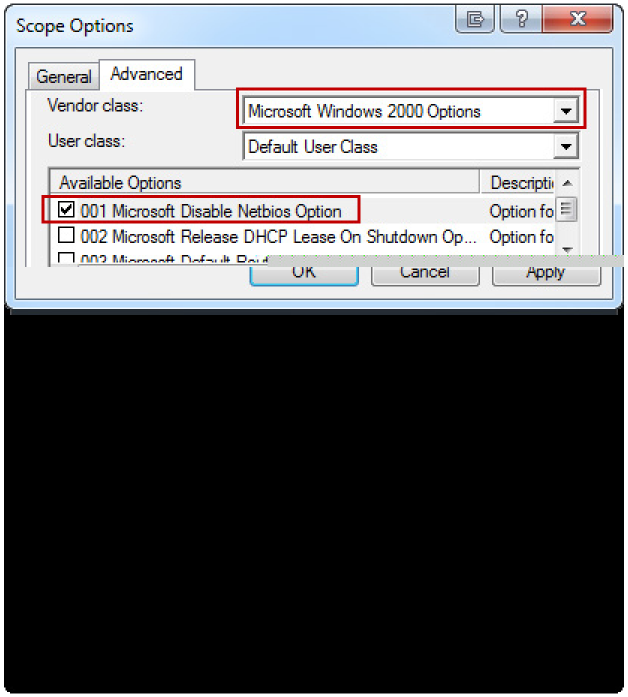
NetBIOS setting

○ Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

● Disable NetBIOS over TCP/IP

OK Cancel



Scope Options

General | Advanced

Vendor class: Microsoft Windows 2000 Options

User class: Default User Class

Available Options	Descripti
☑ 001 Microsoft Disable Netbios Option	Option fo
☐ 002 Microsoft Release DHCP Lease On Shutdown Op...	Option fo
☐ 003 Microsoft Default Rou	

OK Cancel Apply

3 | DISABLE WEB PROXY AUTO-DISCOVERY

Web proxy auto-discovery (WPAD) is an internet setting that automatically goes out and looks for a web proxy server somewhere on the network and configures it for use. WPAD is one of the settings boxes in Internet Explorer that is automatically checked by default. By abusing WPAD requests, attackers can intercept plain text and attempt to decrypt encrypted web traffic. This is a feature that exists in Windows, Linux and Mac browsers, but almost every network does not need it.

If you are using a web proxy server on your network for a legitimate purpose, then send that one out statically instead of using this dynamic service to look for it. The reason behind this approach is that an attacker can deploy a rogue proxy server and attempt to mount a man-in-the-middle attack.

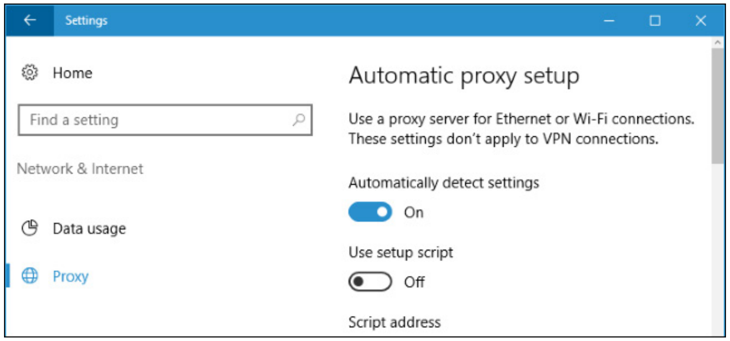
In this scenario, a hacker establishes a system in your environment that will broadcast itself as a web proxy server and the web proxy auto-discovery will associate with that and route any web traffic through that man-in-the-middle, rogue system. Some of the information captured by the hacker will be clear text and in other cases it will be encrypted but can be decrypted later.

As an example, a hacker could easily mount a man-in-the-middle attack against someone using a laptop in a coffee shop, thinking they were using a legitimate web connection, to steal credentials or other sensitive information.

It's simple to stop and disable the WinHTTP WPAD service on all Windows systems. This can be accomplished by disabling WPAD by GPO or manually turning the feature off on non-Windows systems. Just in case, it's recommended to create your own dummy entry in the domain name servers (DNS).

The only amount spent to disable WPAD will be a little diligence looking into every system to make sure this feature has been turned off, and then a simple DNS entry to catch any systems that may have slipped through the holes.

Disabling the WPAD configuration will look like the below images. In Windows, there's a spot where you can have it automatically detect settings—it might be a checked box or could be a slider setting depending on your version of Windows.



Automatic proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

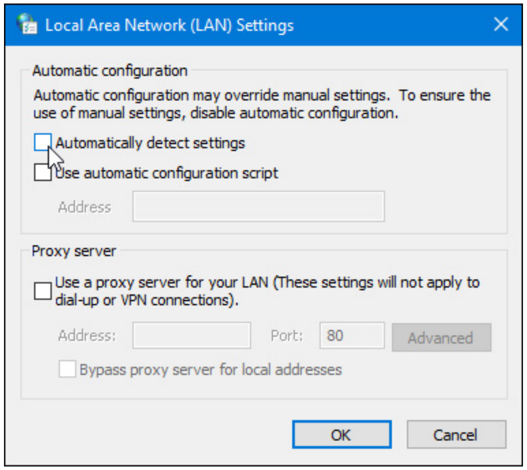
Automatically detect settings

● On

Use setup script

○ Off

Script address



Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

□ Bypass proxy server for local addresses

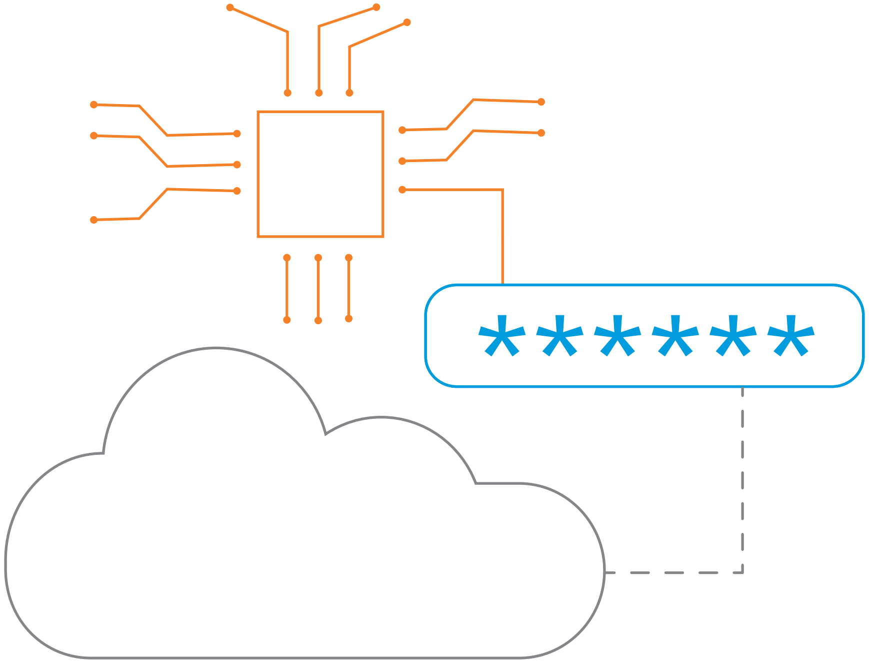
4 | CHANGE DEFAULT CREDENTIALS

Every single device on your network should be secured, because even the most seemingly benign device can be used by the bad guys. Well-known to hackers, many devices come with a default username and password set by the manufacturer. Hackers also have access to lists of the most commonly used custom passwords.

Additionally, IP-based systems like printers, multifunction devices, uninterruptable power supplies, cameras, power distribution units, out-of-band management systems, thermostats, environmental monitors, web cameras and telephony devices can all be used by hackers. These devices are all part of the internet of things, but we don't often think of them as a potential tool for hackers or a place where they could live for months before making a lateral movement throughout the network.

To protect your organisation from these hackers, make a list of all the devices on the network and run a network scan if needed. Next, change the default credentials to unique, complex passwords and unique usernames, if possible. You might be surprised by how many seemingly clever passwords are found on a list floating around on the dark web—from keyboard combinations users think are cute to characters from a popular TV series. In addition, consider segregating devices based on roles for additional access control.

Changing default credentials will require a little time and some legwork, but it won't cost a dime. If you purchase a device that attaches to your network, consider using reputable vendors.



5 | REMOVE LOCAL ADMINISTRATIVE RIGHTS

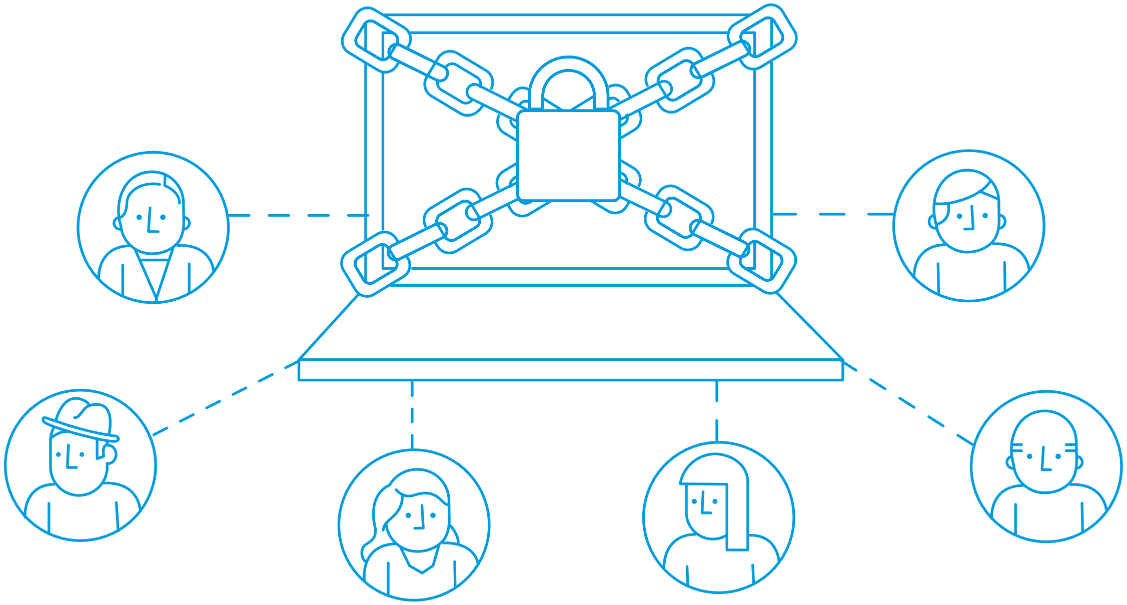
Although sometimes tough for middle market companies, users should never have administrative (admin) rights to their workstations. If a hacker can gain access on behalf of the user through a social engineering attack for example, they will then instantly have local admin access on the entire system. This is another case where a hacker could use an access point as the launching place for a lateral move throughout the whole network.

Additionally, if a hacker compromises admin rights and gains access to a workstation of an employee who has elevator credentials then they can pull up the Windows cache of the credentials to gain domain-wide access to the local system. Also, even from a nonsecurity standpoint, just the general care of your workstations and network will benefit from limiting general admin rights and potential for users to inadvertently do something wrong that must be cleaned up later.

Some software vendors claim that local admin rights are required, but usually they are not. These vendors will recommend giving users access to everything to make it easier and not worry about what they need, but this could backfire in a few scenarios already described.

To fix this issue, all you need to do is change the permissions on all Windows systems and revoke local admin rights from users. If you have any software that requires these rights, determine the minimum specific granular rights the user needs to run the software without giving them local admin rights—maybe the user only needs right permissions to a specific folder or one file.

There's no expense to make this change. It just might take a little time to surgically tweak permissions without using the sledgehammer local-admin approach some software vendors prefer.



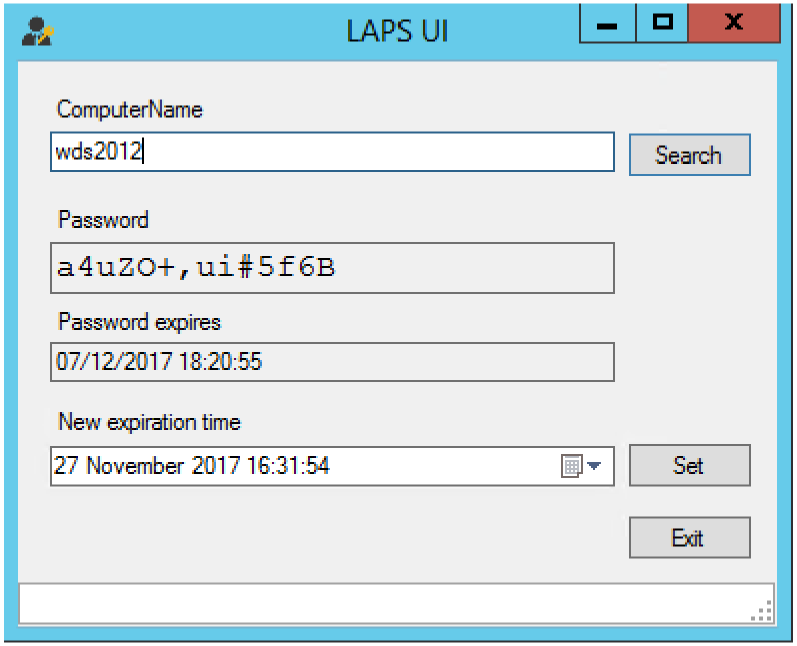
6 | SET UNIQUE LOCAL ADMIN PASSWORDS

Every member server or workstation system has a local admin account and most network admins have a favorite local admin password that is used on several or even all the systems in the environment. This may seem like an easy approach, but if just one workstation or the network is compromised, the hacker now has keys to the whole kingdom. With access to a whole host of systems, it won't be long before they get the information or credentials that they were looking for when they launched the attack.

A local admin password should be on each system that is unique from all the other ones. This can be accomplished in two ways—the hard way which is to set unique local admin passwords on all systems, or the easy way which is to deploy and configure the Microsoft local admin password solution (LAPS) on an existing utility server.

LAPS is a free Microsoft solution and if you deploy it on an existing Windows utility server, there are no licensing costs. There may be a little bit of work to set this up, but it will then quickly provide unique passwords throughout your system and you will be able to prevent one very common avenue for hackers.

The below image shows what the LAPS user interface looks like when you open it. Simply put in a computer name, LAPS will search for it and display the current password.



ComputerName
wds2012

Password
a4uZO+,ui#5f6B

Password expires
07/12/2017 18:20:55

New expiration time
27 November 2017 16:31:54

7 | UPDATE POWERSHELL

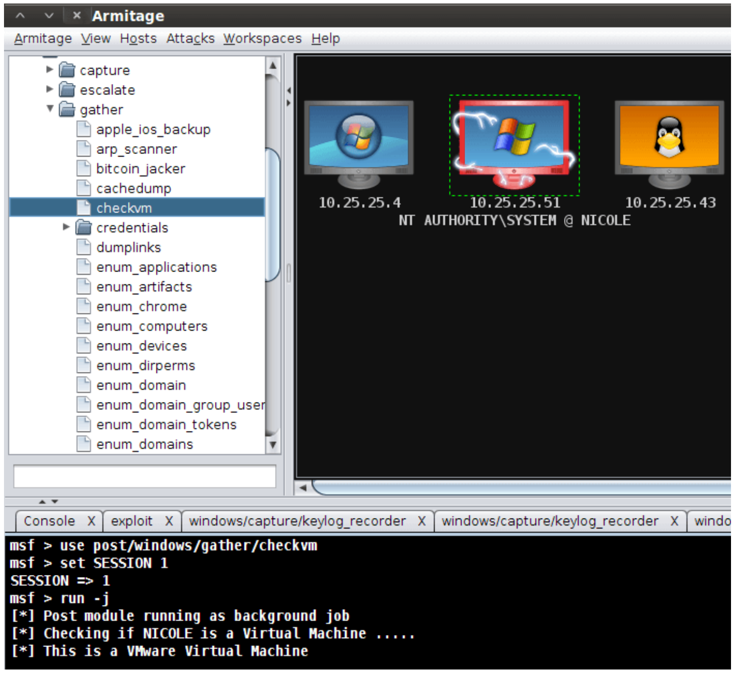
PowerShell 4.x is installed on many systems such as Windows 2012 by default. Windows 8 and older operating systems have PowerShell version 4 or a previous version installed.

Several remote exploits against these versions of PowerShell are available to "script kiddies" through easy-to-use, point-and-click hacking tools. The same hacking platform is also sometimes used by penetration (pen) testers. These tools allow a hacker or pen tester to remotely execute code, dump credentials, modify files and open up connections.

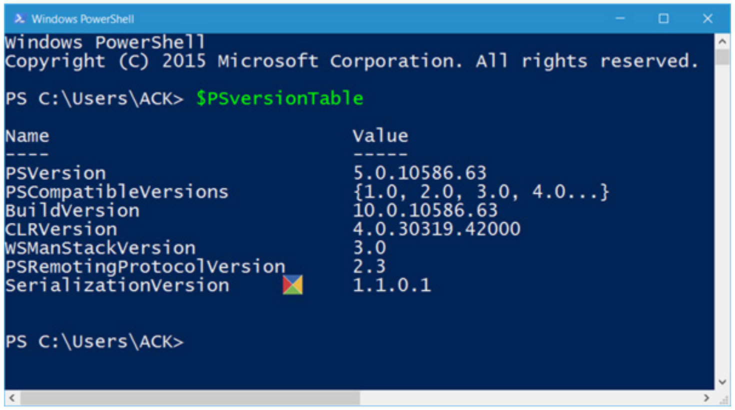
The best step you can take is to update to the latest version of PowerShell 5.x or configure any other monitoring tool you have already to keep a close eye on PowerShell operations and be alerted if something strange is going on.

PowerShell can be updated at no cost and eliminate one more place where pen testers will have an easy job or where the bad guys can do harm. If you are unsure which version of PowerShell you have, you can issue a command when it is opened to view whether it's 4.0, 5.0 or newer.

The following image is an example of an easy-to-use, point-and-click tool that hackers can use to exploit PowerShell. The icon with the red border and lightning bolts around it shows that someone has been able to take control of that system using a PowerShell exploit.



```
msf > use post/windows/gather/checkvm
msf > set SESSION 1
SESSION => 1
msf > run -j
[*] Post module running as background job
[*] Checking if NICOLE is a Virtual Machine .....
[*] This is a VMware Virtual Machine
```

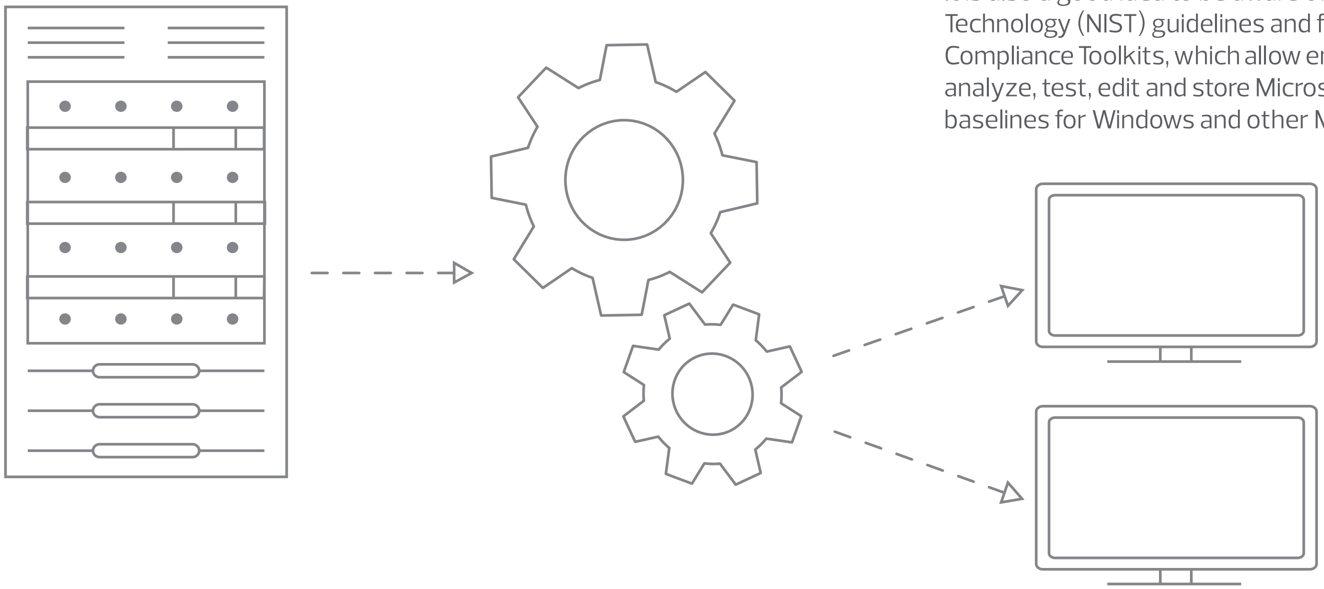


```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\ACK> $PSversionTable

Name                           Value
----                           -----
PSVersion                      5.0.10586.63
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.10586.63
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1


PS C:\Users\ACK>
```

8 | HARDEN YOUR HOSTS

Almost all hypervisors are installed with default security settings and little is usually done to make them more secure. Today's hypervisors have a wealth of options that we usually don't set or in some cases even know about or understand what they do, but many of these settings can help improve the overall security posture.

The hypervisor vendors provide some great information on how to harden the hosts, storage connections, virtual networking, management systems and virtual machines.



Follow the guides provided by the hypervisor vendors at the below links:

- https://www.vmware.com/security/hardening-guides.html
- https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/plan-hyper-v-security-in-windows-server

The guides are extensive, and it might take a little reading and a maintenance window here or there, but you should be able to do this without any need for a budget. With some planning and scheduled maintenance windows, it will be easy to harden both your internal- and external-facing hosts.

It is also a good idea to be aware of National Institute of Standards and Technology (NIST) guidelines and free tools such as Microsoft's Security Compliance Toolkits, which allow enterprise security administrators to download, analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products.

9 | PROTECT YOUR STORAGE

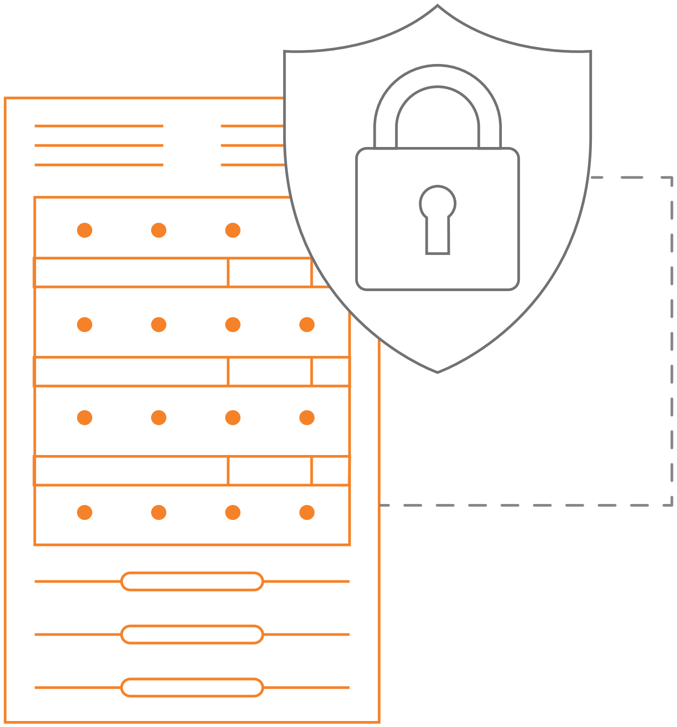
When storage area network (SAN) and network attached storage (NAS) devices are used in an environment, it is important to make sure they have basic protection and isolation from the rest of the network. SAN or NAS storage is available over the network so it is important to isolate these systems and make them only accessible (even via ping) by the hosts that need access.

For example, if you have a storage platform with three hosts connected to it, the storage platform and three hosts are the only systems that should be able to ping on that network. From a networking standpoint, that is called a layer two network where there is no gateway address and it is isolated on an IP range that doesn't cross over to any other network segments.

Additional and free protection is available through Challenge Handshake Authentication Protocol (CHAP) to iSCSI SAN systems. Isolation through physical separation or layer two, virtual local access network (VLAN) segmentation should be used for all IP-based storage network traffic.

To protect your storage, turn on CHAP, host/storage firewalls or any other features you have available to enhance storage security. Next, spend some time identifying where storage traffic is exposed and segment traffic on separate physical switches or nonroutable layer two VLANs.

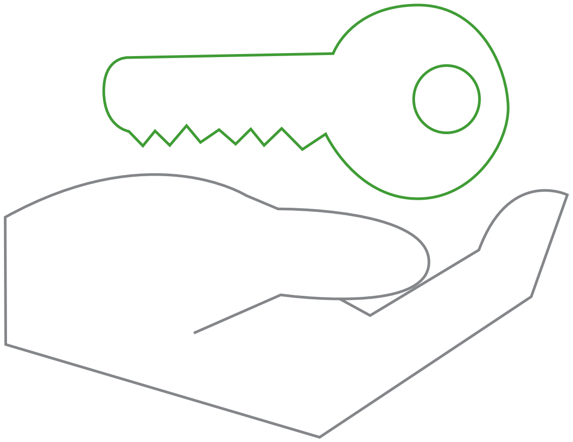
You may need to move a few things around, configure a network port or two, or turn on some features you already own, but you won't need to be signing any purchase orders for this update.



10 | ADOPT A LEAST PERMISSIONS APPROACH

A common approach seen in most industries today is to give users full permissions to everything across the board and then reduce their rights from there. However, a least permissions approach starts with users having no permissions or only giving them the minimum permissions to the resources they need.

Unfortunately, a user's permissions can be used against the company during an attack involving social engineering, ransomware or other methods. In the case of a ransomware attack where a user's permission perpetuates the ransomware spread and they have general permissions to a host of files, their credentials will be used by the hacker to access those files and find information that can be monetized on the dark web.



To help reduce this risk, most users should have rights to a very limited set of files and even fewer folders, if any at all. If they only have access to a very limited set of files, there's a much smaller number of files to worry about if there is a ransomware attack or something else happens.

An audit of new technology file system (NTFS) permissions on all systems and file servers should be conducted and permissions should then be updated using the least permissions approach. Whenever a user has permissions to a file or folder, carefully consider if the permissions are appropriate or not. Reining in the use of "everyone" or "authenticated users" or "domain users" is also recommended when it comes to giving write permissions to bigger user umbrella groups.

This approach won't cost a dime but can be a large undertaking depending on your file structure and size. Rest assured, your hard efforts will pay off, especially when your company isn't unfortunate enough be the victim of a ransomware breakout.

11 | VERIFY BACKUP INTEGRITY

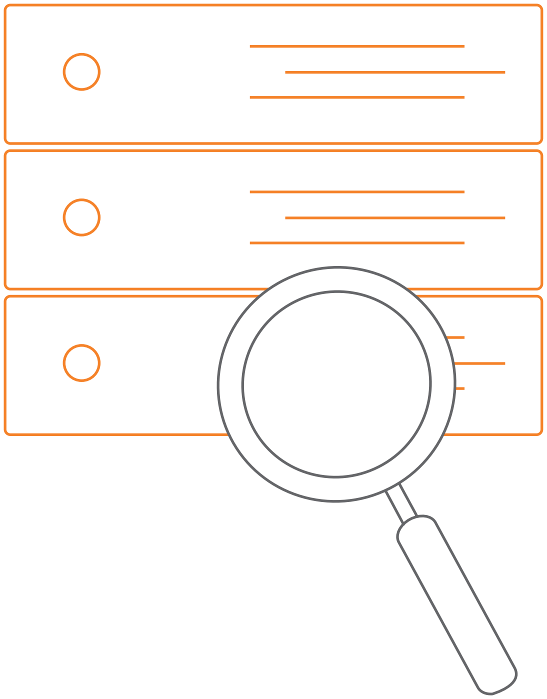
Not surprisingly, backups are a frequent target of attackers because unencrypted data stored within online backups is easy for unencumbered exfiltration. Recent ransomware variants have been known to first attack online backup files to force companies into paying ransom for the return of data.

A common example is a database that is only backed up for flat files periodically, to allow quick restores. These systems are typically unencrypted and stored on a regular unencrypted file server, and, therefore, easy targets for an attacker.

Backups should be stored as offline as possible and domain credentials should not be used to access backup repositories—use storage-based snapshots instead whenever possible. Also, backups of databases or other applications regularly taken through maintenance plans or other mechanisms apart from the enterprise backup solution should be stored encrypted in order to maintain the integrity of the core system.

Next, it's important to verify that your backups are impervious to attack or compromise. Think about what could happen if the entire domain is unavailable, or domain admin permissions have been compromised. If you suspect that an attacker could get to your backups, then you need to update the system's design.

Verifying your backup integrity has no cost to it. Just take a fresh look at how your backups are being stored and identify what the worst-case scenario would be if a hacker gets access to your environment.



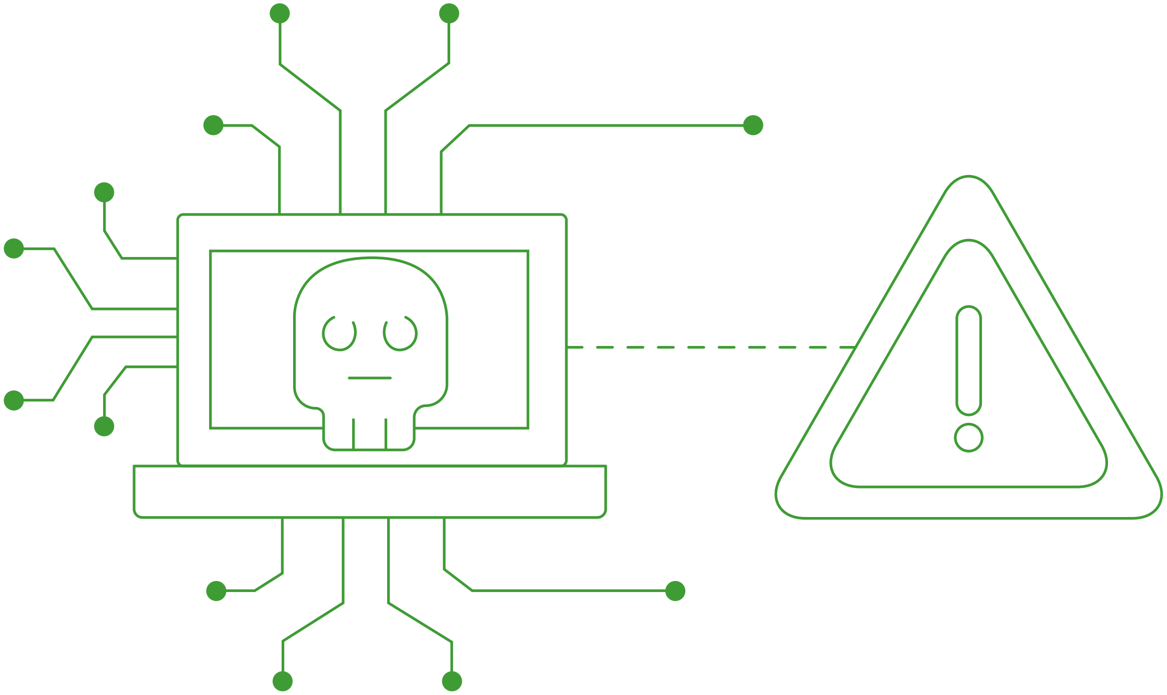
12 | AGGRESSIVELY PATCH EVERYTHING

Always assume that everything on your network is a potential target. Likewise, everything on the network can and should be frequently updated and patched.

All unpatched systems, not just Windows patches, are the top vulnerability for exploits by hackers. Many companies don't regularly patch non-Windows software including Adobe, Flash, Java, etc. or hardware such as switches, printers, etc.

Develop a regular patching schedule and patch everything on the network that is identified through an IP scan. Also, look for methods to always keep ancillary software up to date. If a device or software cannot be patched, then it needs to be removed from your environment immediately.

If you're maintaining support on current systems, the vendors should provide updates and patches without a charge. It just takes some work as well as a process to keep everything up to date and running smoothly.



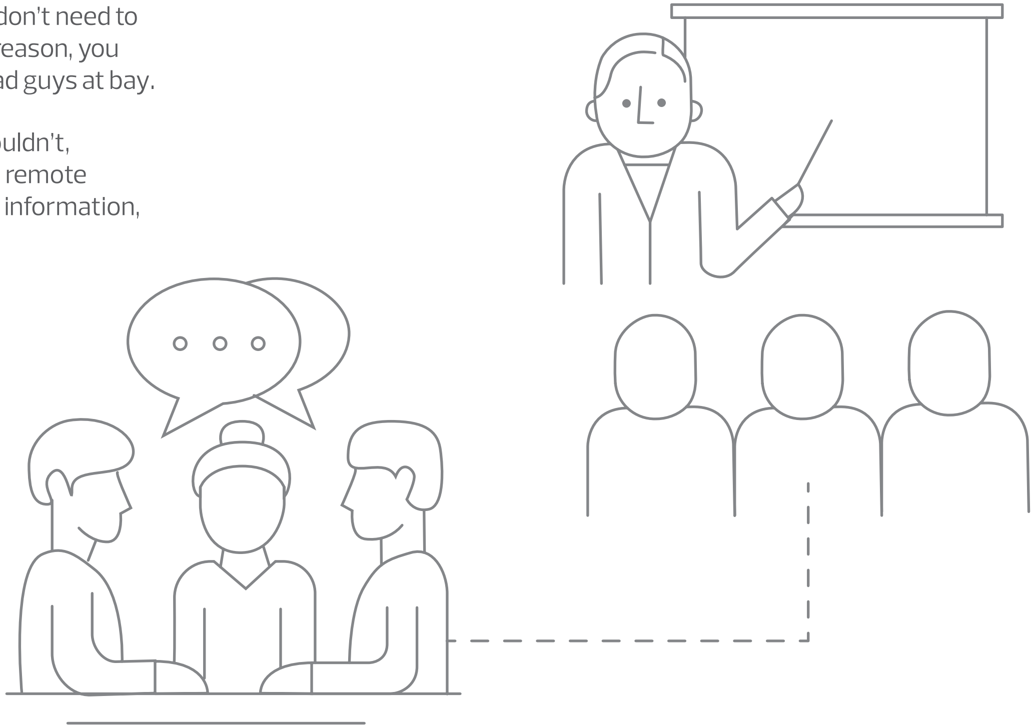
13 | EDUCATE YOUR USERS

Social engineering is the favorite tool of lazy hackers because they don't need to do the work if they can get someone else to do it for them. For this reason, you must arm your users with the training and awareness to keep the bad guys at bay.

Unfortunately, users are often tricked into taking actions they shouldn't, whether it's clicking on a rogue link, opening an infected file, giving remote access to an internal system, transferring funds, sending sensitive information, or even letting a stranger into the company.

Use your existing training material and double-down on your user training. Make cyber security a top issue at your company and lead the charge. Test your users often—once a year is not frequent enough if you want them to be hypervigilant and hyperaware of suspicious activity that comes their way via email or phone. Also, celebrate success by posting results of your tests in your newsletter or in the breakroom and show examples of how users have helped thwart potential hackers.

There's no need to invest in new training programs—use what you have and use it a lot. Make cyber security the number one topic at your organisation and eventually your users will get on board and be your best first line of defense.



14 | USE DATA-AT-REST ENCRYPTION

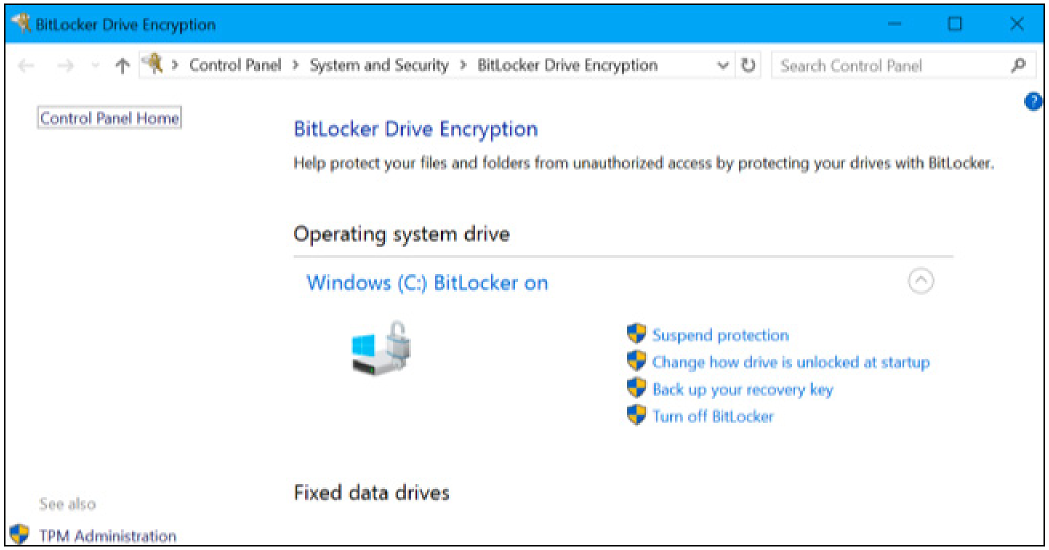
Data stored on hard drives is susceptible to loss by theft, or even vulnerable when simply returning a failed drive or device for warranty replacement. To substantially reduce this risk, data-at-rest encryption tools can be used to store all data in encrypted files when sitting on a hard drive or solid-state drive (SSD). Encryption is available on SAN/NAS systems, servers, desktops, laptops, etc.

Lost, stolen or warranty-returned media will not contain recoverable information if it is protected with data-at-rest encryption. These technologies are becoming more of a standard and a must-have in regulated industries.

To get started, check your SAN/NAS for data-at-rest encryption capabilities and turn it on if it is available. Next, configure and enable BitLocker on all Windows desktop and laptop systems.

You will most likely already have these tools available and it's just a matter of turning them on. If you don't have them, as you naturally replace hardware when it ages out, make sure the new systems do have this feature.

Below is an example of what BitLocker looks like, which is available on most newer Windows-based operating systems to easily encrypt your hard drive.


BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home
See also
TPM Administration

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows (C:) BitLocker on

- Suspend protection
- Change how drive is unlocked at startup
- Back up your recovery key
- Turn off BitLocker

Fixed data drives

15 | TAG EXTERNAL AND SUSPECT EMAIL MESSAGES

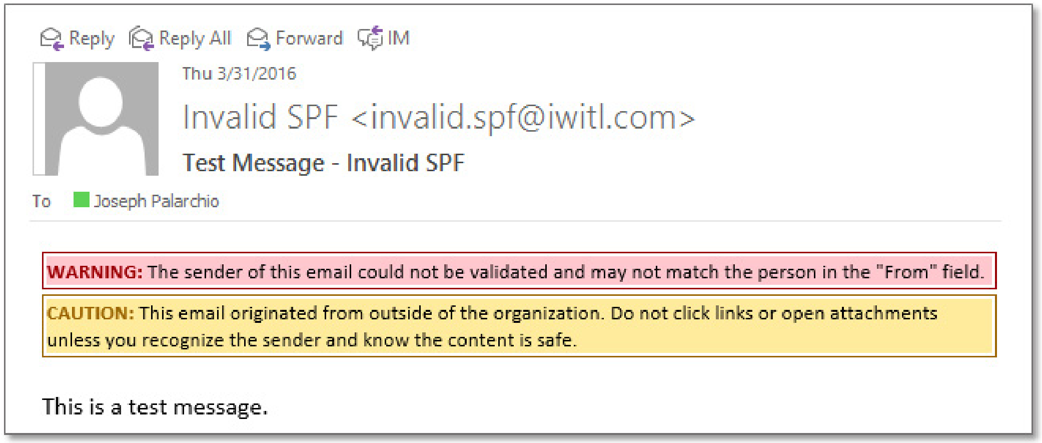
Last but by no means least, email spoofing and business email compromise have become prominent forms of attack in recent years. An example could be a hacker getting into executives' emails, learning how and when they communicate, and then waiting until just the right moment to put in a request to a colleague to transfer funds to an offshore account.

Providing your users with a clear and obvious warning that emails are from external or suspect sources will help them make good decisions and again make them part of an effective first line of defense for your organisation. The most common email systems we use today have built-in tools to help with this detection.

Microsoft Exchange and Microsoft Office 365 both contain options to detect email coming from outside the organisation. Sender policy framework (SPF) provides a check to ensure an external email came from a server that is authorized to send on behalf of that domain. Microsoft Exchange and Microsoft Office 365 can check the SPF record and warn if an email is coming from an unauthorized server, indicating it may be fraudulent or spoofed.

Configure your email server to clearly and obviously notify users whenever they receive an external email. Additionally, configure your email server to check for SPF records and provide a clear and obvious warning for any email that was sent with an unauthorized email server.

This can all be set up without spending a dime—simply create some rules on your email server(s) and provide your users with training on what to do if they see a header (image below) alerting them to an invalid email.



Thu 3/31/2016

Invalid SPF <invalid.spf@iwitl.com>

Test Message - Invalid SPF

To 🟩 Joseph Palarchio

WARNING: The sender of this email could not be validated and may not match the person in the "From" field.

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

This is a test message.

THE COMPLETE CHECKLIST

Below is a checklist of the 15 steps you can take today, none of which cost a dime, that will help improve your cyber security posture. This is not an exhaustive list and the activities outlined in this e-book should be used in concert with other strategies to safeguard the integrity of your systems.

Cyber security checklist

- □ Disable local link multicast name resolution (LLMNR)
- □ Disable NetBIOS name services (NBT-NS)
- □ Disable web proxy auto-discovery
- □ Change default credentials
- □ Remove local admin rights
- □ Set unique local admin passwords
- □ Update PowerShell
- □ Harden your hosts
- □ Protect your storage
- □ Adopt a least permissions approach
- □ Verify backup integrity
- □ Aggressively patch everything
- □ Educate your users
- □ Use data-at-rest encryption
- □ Tag external and suspect email messages

Again, it is important to note that most security systems and initiatives do have associated costs—and must be budgeted for and funded. A trusted advisor can help your organisation design, implement and maintain security architectures that safeguard your network, data and client files.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

rsm.com.au

RSM