Maner Costerisan
Certified Public Accountants
Business & Technology Advisors

IT Security

Protecting your organization from the inside out

Joe DeLuca
jdeluca@manersolutions.com

Ryan Carter
rcarter@manersolutions.com

Introduction

Attacks against computing infrastructures, whether simple or complex, have existed as long as computers have. However, within the past decade, increasing numbers of organizations of all sizes, in all parts of the world have been attacked and compromised in ways that have significantly changed the threat landscape.

Cyber-warfare and cybercrime have increased at record rates. "Hacktivism," in which attacks are motivated by activist positions, has been claimed as the motivation for a number of breaches intended to expose organizations' secret information, to create denials-of-service, or even to destroy infrastructure.

Attacks against public and private institutions with the goal of exfiltrating the organizations' intellectual property (IP) have become ubiquitous.

Maner Costerisan
Certified Public Accountants
Business & Technology Advisors

Intacct Partner

socius

Microsoft Partner

No organization with an information technology (IT) infrastructure is immune from attack, but if appropriate policies, processes, and controls are implemented to protect key segments of an organization's computing infrastructure, escalation of attacks from penetration to complete compromise might be preventable.

While the number and scale of attacks originating from outside an organization has eclipsed insider threat in recent years, the principles and recommendations provided are intended to help secure your environment against misguided or malicious insiders as well as external attackers.

Maner Costerisan

Intacct Partner

sociUS

Microsoft Partner

Although it is not possible to prevent attacks, it is possible to reduce the attack surface and to implement controls that make compromise much more difficult for attackers.

Our session today presents some of the most common types of vulnerabilities we have observed in compromised environments and the most common recommendations we have made to our clients to improve the security of their organizations.

Maner Costerisan

Intacct Partner

sociUS

Microsoft Partner

User Accounts

Let's face it. Users are the weakest link in any network security scenario. But since they are also the reason we have IT and more to the point…**a job**…we need to make sure we take care of them and they take care of us. That's why they come first on this list.

Training

Before a user ever gets a network account, they need training on what to do, what not to do, and how to go about protecting themselves and the network. This needs to be done first, and repeatedly, with at least an annual review and update.

Separating normal/privileged user accounts

This goes without saying, but make sure you log on with a regular account, and only authenticate with a privileged account when you need to do admin work.

You never know when you might accidentally click something that runs with those elevated privileges.

Multifactor authentication

If you look at every major hack that has hit the news in the past couple of years, from T.J. Maxx to Target to Premera to the Office of Personnel Management…one thing could have prevented them all. Two factor authentication.

Every one of those hacks started with compromised credentials which were simply username and password.

Review of group memberships when roles change

Given least privilege, it must be standard operating procedure to review and revise group memberships and other access privileges when a user changes jobs. If their new role does not require access to resources that their old role gave them, remove that access.

No sharing of accounts between test and production, or between any two external services

This one is critical. If you have multiple environments it may be very tempting to share credentials between them.

That makes it much more likely that compromise can occur, especially if the lab or UAT environment doesn't have the same security measures as production does, or that the hack of one external service could reveal your credentials that could then be used to log onto other services.

POP QUIZ!

Is your username and password for Facebook the same as for Twitter?

If you answered yes, you're doing it wrong.

Disable stale accounts. Delete the really old ones.

This powershell script searches a specified OU tree in AD for accounts that have been disabled longer than a certain period of time and then deletes them. User accounts can be whitelisted from the cleanup process and once complete, the script compiles a nice HTML report and emails it to IT staff. The report includes accounts deleted, which accounts will be deleted on the next run, whitelisted accounts, and any other disabled accounts in the OU tree so staff can see which ones are coming up on the deletion time.

https://gallery.technet.microsoft.com/scriptcenter/Disabled-AD-Account-8cc92a7d

Policies

The best laid plans of mice and men oft go awry, and nowhere can this happen more quickly than where you try to implement network security without a plan, in the form of policies.

Policies need to be created, socialized, approved by management, and made official to hold any weight in the environment, and should be used as the ultimate reference when making security decisions.

- Acceptable Use Policy
- Internet Access Policy
- Email and Communications Policy
- Network Security Policy
- Remote Access Policy
- BYOD Policy
- Encryption Policy
- Privacy Policy

A great resource for policy starter files and templates is the SANS Institute at http://www.sans.org

Maner Costerisan
Intacct Partner
sociUS

Servers

If you were to ask a bank thief why s/he robs banks, the likely answer is because that's where the money is.

If you could ask a hacker why s/he breaks into servers they would probably reply with a similar answer…

'because that's where the data is'

Naming conventions

Naming conventions may seem like a strange thing to tie to security, but being able to quickly identify a server is critical when you spot some strange traffic.

If an incident is in progress, every second saved counts.

Maner Costerisan
Intacct Partner
sociUS

Responsible party

Each server must have a responsible party; the person or team who knows what the server is for, and is responsible for ensuring it is kept up to date, and can investigate any anomalies associated with that server.

Make sure to update this when people change roles.

IP Address Management

All servers should be assigned static IP addresses, and that data needs to be maintained in your IP Address Management tool (even if that's just an Excel spreadsheet.)

When strange traffic is detected, its vital to have an up to date an authoritative reference for each IP address on your network.

Windows Server 2012 R2 includes IPAM services.

Patching

Every server deployed needs to be fully patched as soon as the operating system is installed, and added to your patch management application/schedule immediately.

Antivirus

All servers need to run antivirus software and report to a central management console.

Scanning exceptions need to be documented in the server list so that if an outbreak is suspected, those directories can be manually checked.

Maner Costerisan
Intacct Partner
sociUS

Correct OU with appropriate policies

Different servers have different requirements, and Active Directory Group Policies are just the thing to administer those settings.

Create as many OUs as you need to accommodate the different servers, and set as much as possible using a GPO instead of the local security policy.

Backups

If it's worth building, it's worth backing up.

No production data should ever get onto a server until it is being backed up.

'Backups are just slightly less important than your heartbeat.'

Maner Costerisan
Intacct Partner
sociUS

Restores

And no backup should be trusted until you confirm it can be restored.

Vulnerability scan

If you really think the server is ready to go, and everything else on your list has been checked off, there's one more thing to do; scan it.

Run a full vulnerability scan against each server before it goes into production to make sure nothing has been missed, and then ensure it is added to your regularly scheduled scans.

Group Policy

Security through obscurity

A method in which parts of the user experience are hidden, or obfuscated, to prevent access to features within the operating system

Hardening vs lockdown

- Hardening – Process of securing a system by reducing its surface of vulnerability
- Lockdown – Process of securing the subsystems and applications that run on top of the operating system

Maner Costerisan
Intacct Partner
sociUS

Hardening your OS

- Programs clean-up – Remove unnecessary programs. Every program is another potential entrance point for a hacker. Cleaning these out helps you limit the number of ways in. If the program is not something which has been vetted and "locked down," it shouldn't be allowed. Attackers look for backdoors and security holes when attempting to compromise networks. Minimize their chances of getting through.
- Use of service packs – Keep up-to-date and install the latest versions. It's that simple. No one thing ensures protection, especially from zero-day attacks, but this is an easy rule to follow.
- Patches and patch management – Planning, testing, implementing and auditing patches should be part of a regular security regimen. Make sure the OS is patched regularly, as well as the individual programs on the client's computer.

- Group policies – Define what groups can or can't access and maintain these rules. Sometimes, it's simply user error that leads to a successful cyber attack. Establish or update user policies and ensure all users are aware and comply with these procedures. For example, everyone should be implementing strong passwords, securing their credentials and changing them regularly.
- Security templates – Groups of policies that can be loaded in one procedure; these are commonly used in corporate environments.
- Configuration baselines – Baselining is the process of measuring changes in networking, hardware, software, etc. To create a baseline, select something to measure and measure it consistently for a period of time. Establish baselines and measure on a schedule that is acceptable to both the standard for maintaining security and meeting your organizations' needs.

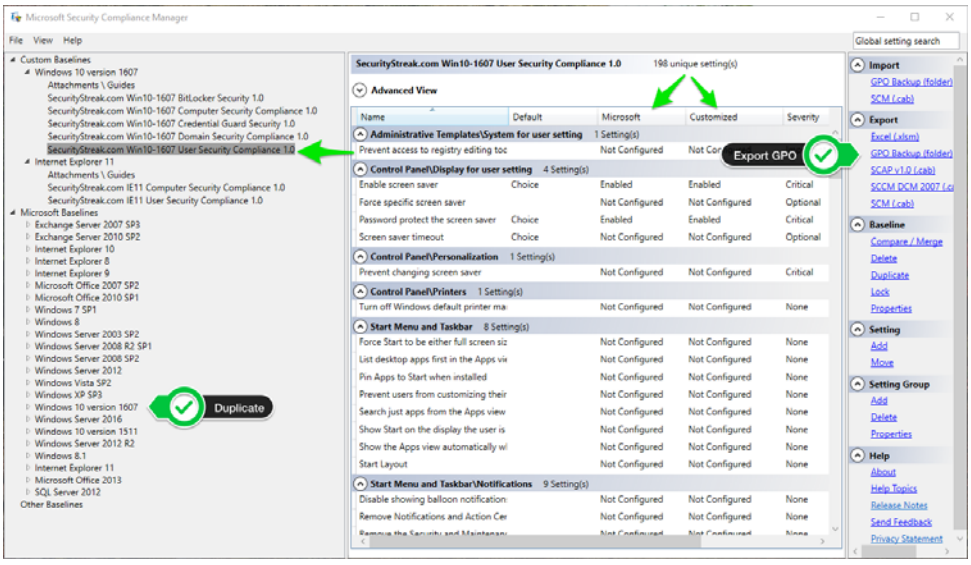
Maner Costerisan
Intacct Partner
socius

Establish your baselines

Microsoft Security Compliance Manager

The Security Compliance Manager (SCM) is a free tool from Microsoft that enables you to quickly configure, and manage the computers in your environment using Group Policy and Microsoft System Center Configuration Manager.

- https://www.microsoft.com/en-us/download/details.aspx?id=53353



Firewall – Traditional vs Next Generation

A traditional firewall, as it is currently defined, includes a device that is able to control the traffic that is allowed to enter or exit a point within the network. It can typically do this either using a stateless method or a stateful method depending on the type of protocol being run on it.

Next Generation Firewalls do everything the traditional models can do, plus:

- Application Awareness
- Stateful Inspection
- Integrated Intrusion Protection System (IPS)
- Identity Awareness (User and Group Control)
- Bridged and Routed Modes
- And the ability to utilize external intelligence sources

P.S.

Network hardware such as a firewall uses an operating system too, we just call it firmware.

Keep up to date on patches and security updates for your hardware.

More best practices

SNMP - If you are going to use SNMP, change the default community strings and set authorized management stations. If you aren't, turn it off.

Split tunneling - Protect your travelling users who may be on insecure wireless networks by tunneling all their traffic through the VPN instead of enabling split tunneling.

Remove everyone and authenticated users

The default permissions are usually a little too permissive. Remove the Everyone group from legacy shares, and the authenticated users group from newer shares, and set more restrictive permissions, even if that is only to “domain users.” This will save you a ton of time should you ever have to set up a share with another entity.

Local encryption

There is no excuse for letting any laptop or portable drive out of the physical confines of the office without encryption in place to protect confidential data. Whether you use Bitlocker, third party software, or hardware encryption, make it mandatory that all drives are encrypted.

BYOD

Create a “Bring Your Own Device” policy now, even if that policy is just to prohibit users from bringing their personal laptops, tablets, etc. into the office or connecting over the VPN.

Wireless

Encryption

Use the strongest encryption type you can, preferable WPA2 Enterprise. **Never** use WEP.

If you have bar code readers or other legacy devices that can only use WEP, set up a dedicated SSID for only those devices, and use a firewall so they can only connect to the central software over the required port, and nothing else on your internal network.

Guest Network

Use your wireless network to establish a guest network for visiting customers, vendors, etc.

Do not permit connectivity from the guest network to the internal network, but allow for authorized users to use the guest network to connect to the Internet, and from there to VPN back into the internal network, if necessary.

SSID

Use an SSID that cannot be easily associated with your company, and suppress the broadcast of that SSID.

Neither are particularly effective against someone who is seriously interested in your wireless network, but it does keep you off the radar of the casual war driver.

E-Mail

Inbound and outbound filtering - Deploy an email filtering solution that can filter both inbound and outbound messages to protect your users and your associates.

Directory Harvest prevention - Ensure that your edge devices will reject directory harvest attempts.

Antivirus/Antispam/Antiphishing - Deploy mail filtering hardware or software that protects users from the full range of email threats, including malware, phishing attacks, and spam.

Most successful attacks don't involve a flaw in the software. Instead, they exploit misconfigurations—for example, permissions that were lowered during troubleshooting but never reset, an account that was created for a temporary employee but never disabled when he left, a direct Internet connection that someone set up without approval, and so forth.

If your procedures are sloppy, it can be difficult or impossible to keep track of these details, and the result will be more holes for a bad guy to slither through.

The most important tool here isn't a software tool—it's procedures.

Having specific, documented procedures is an absolute necessity. It starts with the corporate security policy, which should spell out, at a broad level, who's responsible for each part of the network, and the overall philosophy governing deployment, management and operation of the network. The more specific these procedures are, the better.

And write them down!

If your procedures exist only as oral tradition, they'll be lost as your IT personnel changes.

Maner Costerisan

Intacct Partner

sociUS

Microsoft Partner

Thank you!

Maner Costerisan

Intacct Partner

sociUS

Microsoft Partner