Modernizing Your Cyber Security Approach with the Center for Internet Security

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

©New Net Technologies

INTRODUCTION

Center for Internet Security is primarily known as the information security industry's leading authority on security configuration guidance, developing comprehensive, consensus-derived checklists to help identify and mitigate known security vulnerabilities. CIS Benchmarks are the recommended hardening build-standard for all security and compliance initiatives.

In early 2017, NNT assembled a panel of experts to discuss the increased importance of applying the Center for Internet Security Controls as part of a modern approach to cyber security. The session also highlighted the benefits of combining the CIS Controls with ongoing, real-time compliance monitoring.

Key questions covered during the session included:

- Why are hackers still able to exploit existing known vulnerabilities?
- Why do you need to understand the state of the configuration of your IT estate?
- Why do organizations tend to prioritize focus on perimeter defenses at the expense of the actual systems that store sensitive data?
- What is the latest guidance with respect to Ransomware?
- Why is CIS relevant?
- Eliminating vulnerabilities by hardening comes with a health warning - what is the safest way to do it?

TIME TO MEET THE PANEL

Adam Montville, Center for Internet Security

Adam Montville is the VP Programs and Product Manager at CIS, where he helps lead a team of folks developing products and services supporting information security best practices and automation. Adam brings nearly two decades of information security experience to his team, and is a co-chair for the Security Automation and Continuous Monitoring working group at the IETF. He has held a variety of technical and executive-level IT and security positions in both the public and private sectors, including the Department of Defense

"Despite all of that – he would still much rather be fishing in Montana!"

David Froud, Core Concept Security

David is the Director & Principal Trainer at Core Concept Security. As a Project Lead for several Fortune/FTSE Enterprise Class clients, David has performed hundreds of on site security and compliance assessments for merchants and service providers globally. David is currently focused on helping organizations unify their security programs with upcoming EU regulatory compliance regimes.

"David provides Cyber Security Guidance to over 40 different Countries. All of whom he professes remain equally broken!"

Mark Kedgley, New Net Technologies

As the CTO at New Net Technologies, Mark is the technical lead within the company and is responsible for researching the latest market trends, identifying the technological requirements and translating these points into innovative product functionality.

"Still a terrible tennis player

TO SET THE SCENE...

> *“...breaches happen fast and the damage has been done long before anybody knows anything about it.*
>
> *Better defenses are needed, but faster/real-time breach detection is vital.”*

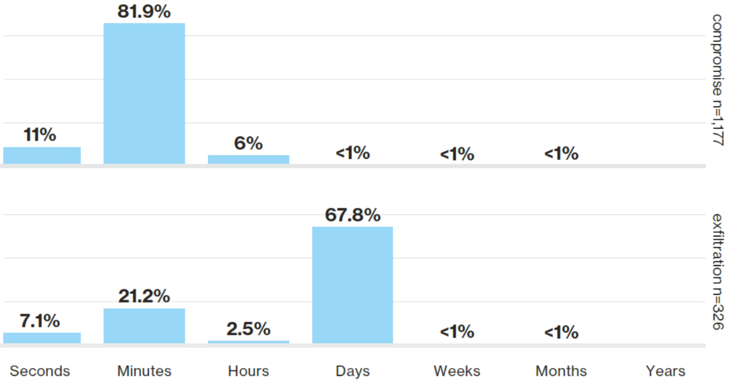
“Its still a tie in the cybersecurity war - the attackers get better resources as quickly as the corporate security team do”

Recent reports show the majority of breaches only need to be active for a period measured in days. One third of these take what they want within minutes, for example user credentials. The rest remain active to steal, for example, payment card data. By contrast, only 25% of breaches are discovered within a comparable period.
So breaches happen fast with damage done long before anybody knows anything about it.
Better defences are needed, but faster/real-time breach detection is vital.

“Why do we seem to be stuck in first gear when it comes to the cybersecurity race?”

Figure 1: The timeline here is in seconds, minutes, hours, days, up to years and shows how fast a breach can be executed and completed.

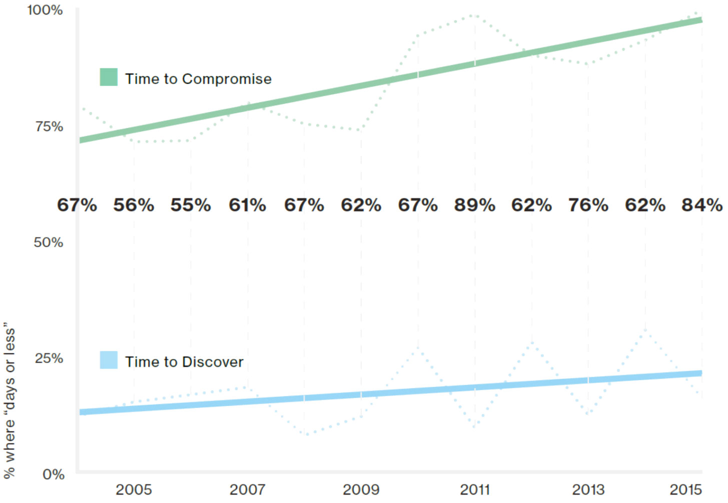
The upper chart shows Time to Compromise - overwhelming majority of breaches take just minutes.



The lower chart shows Time to Exfiltration but there are two ways to look at this because breaches have different objectives - 30% have taken what they want within minutes/hours, for example stealing credentials, while the majority work in the Days category because they are looking to steal data over a prolonged period of time, for example, payment card data.

Figure 2: The lower line shows the percentage of attacks that were discovered within days or less - we are getting slightly better over time, largely due to the insistence of compliance standards that Breach Detection/Integrity Monitoring is used.

The bad news is the top line - this show percentage of attacks where the time to compromise is days or less and as we saw in the previous slide, the majority are effective within hours.



Conclusion is that breaches happen fast and the damage has been done long before anybody knows anything about it. Better defences are needed, but faster/real-time breach detection is vital.

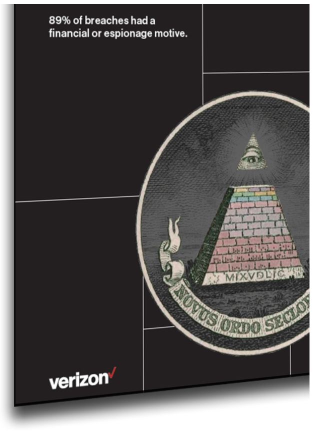


Figure 3: Verizon’s Data Breach Investigations Report for 2016 shows that in cybersecurity terms, the more things change, the more they stay the same.

WHY ARE HACKERS WILL ABLE TO EXPLOIT KNOWN VULNERABILITIES?

Hackers use what works and what works doesn't seem to change all that often.Secondly, attackers automate certain weaponized vulnerabilities and 'spray and pray' them across the internet, sometimes yielding incredible success. The distribution is very similar to last year, with the top 10 vulnerabilities accounting for 85% of successful exploit traffic. How can this be the case?

> "...as the Defender, you need to be right all the time - the Attacker only needs to be right once"

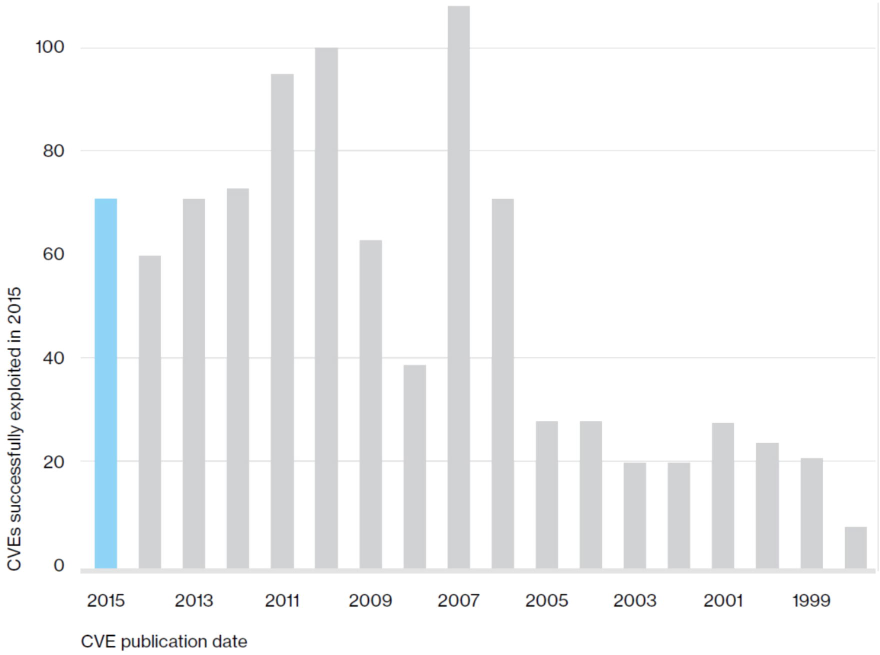


Figure 4: Groundhog Day for breach investigators as 'old news' vulnerabilities are still available and effective

"Because too many of us make it easy for them!" Mark Kedgley kicked things off.

"The most successfully exploited vulnerabilities exist on older abandoned platforms such as Windows XP, with these still widely in use on some of the most lucratively rewarding systems such as Retail POS and banking ATMs.

Only conclusion is that change/cost averse organizations are hanging onto outdated platforms. Unable to move from a legacy platform? The need for hardening and breach detection is even more acute as the only path available to increase security"

David Froud: "For an organization to adjust to the prevailing threat landscape (i.e. vulnerabilities) it demands 4 key things from their security program:

1. they have one in the first place :-)
2. they have robust asset management
3. their vulnerability management program covers all assets, and
4. their incident response processes can fill-in where vulnerability management fails.

Experience shows few organizations have these processes in place - even fewer do them well!"

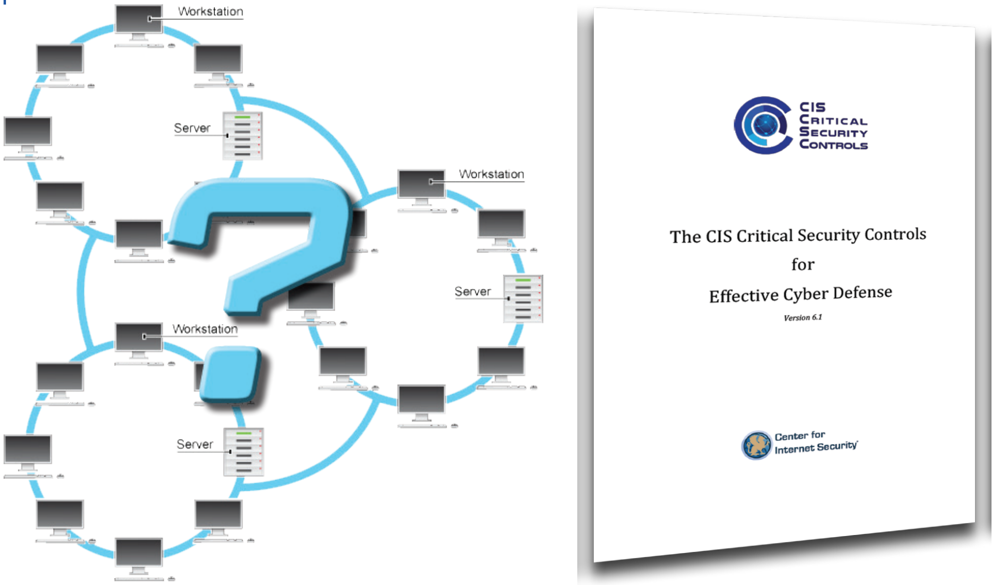
Adam from CIS gave a neat summary of the inequality of the struggle between Defender and Attacker: "The problem is that you, as the Defender, you need to be right all the time - the Attacker only needs to be right once"

WHY DO YOU NEED TO UNDERSTAND THE CONFIGURATION OF YOUR IT ESTATE?

Number One in the CIS Critical Security Controls is ‘Establish an inventory of Authorized and Unauthorized devices’

Is this just a case of ‘You cant manage what you cant measure?’ You can’t secure devices if you don’t even know they are there - or is it really the most important security best practice?

> “... cyber security skill-sets are still in short supply...Too many security vendors sell their clients what they ask for, not what they need”



CIS Critical Security Controls

The CIS Critical Security Controls
for
Effective Cyber Defense
Version 6.1

Center for Internet Security

Figure 5: Groundhog Day for breach investigators as ‘old news’ vulnerabilities are still available and effective

Adam, CIS: “Don’t get stuck boiling the ocean, and focus on the foundational aspects first. The CIS Controls are prioritized for a reason, and if you look at the foundational controls (Controls 1 through 5, plus 11), you’ll get a long way relatively quickly. Things can become complex fairly quickly, so start with a narrowed scope with those systems most critical to your business (i.e. what can’t fail for your operations to continue). Bring in cloud-based services. Account for mobile devices under management and BYOD. These can all be done in iterative phases

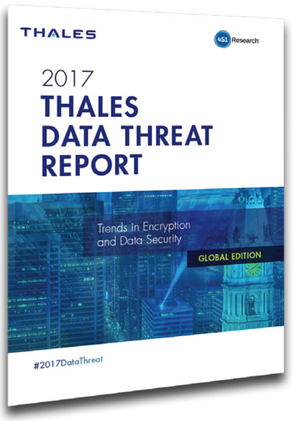
David Froud, Core Concept Security explained his viewpoint: “An inventory of authorized devices’ is the number one Control in the CIS/SANS Top 20 for good reason: You can’t defend what you don’t know you have – you are blind to what your security needs are. Many organizations have functionality expertise when it comes to IT infrastructure, but cybersecurity skill-sets are still in short supply. The cost of in-house security expertise if invariably prohibitive, leaving organizations relying on outsourced providers. Asking the right questions to get the right services is an art form in itself, it takes an expert to hire an expert. Too many security vendors sell their clients what they ask for, not what they need”

Mark at NNT rounded off the answer “First point to make is that if you don’t know what you have today and somebody adds a new device to your network tomorrow, you wont spot it – network sniffer or rogue access point for example.

Your knowledge needs to go beyond the platform, further than the software and versions installed, right through to the actual settings at a security policy-level where config vulnerability mitigation is enabled. Changes here could weaken hardened defences leaving you prone to attack – you need visibility at this level”

WHY DO ORGANIZATIONS TEND TO PRIORITIZE FOCUS ON PERIMETER DEFENSES AT THE EXPENSE OF THE ACTUAL SYSTEMS THAT STORE SENSITIVE DATA?

A survey run by Thales suggests that network spending for security defense is still the number one priority. On one level it makes sense to prevent incursions from the internet, on the other hand, it is the servers and workstations that are actually being targeted, so shouldn't they be the primary focus?



THALES

451 Research

2017 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

GLOBAL EDITION

#2017DataThreat

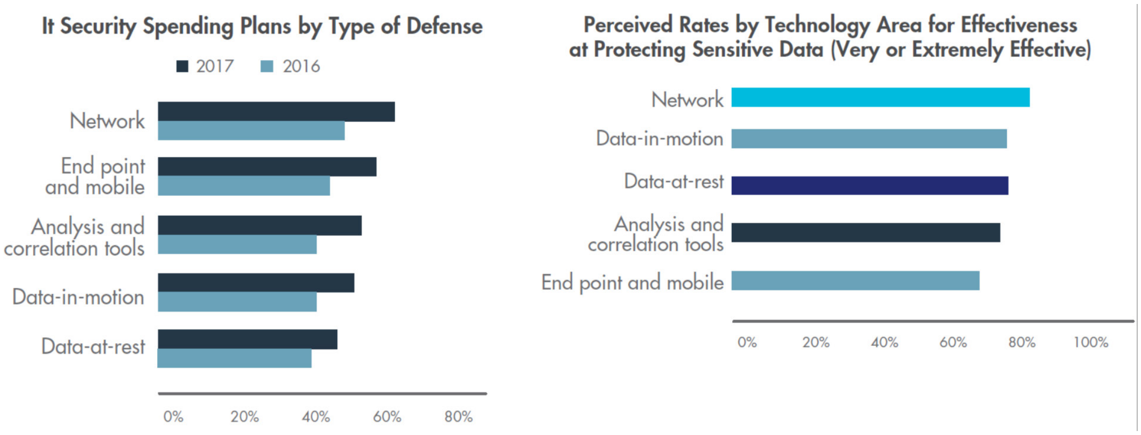
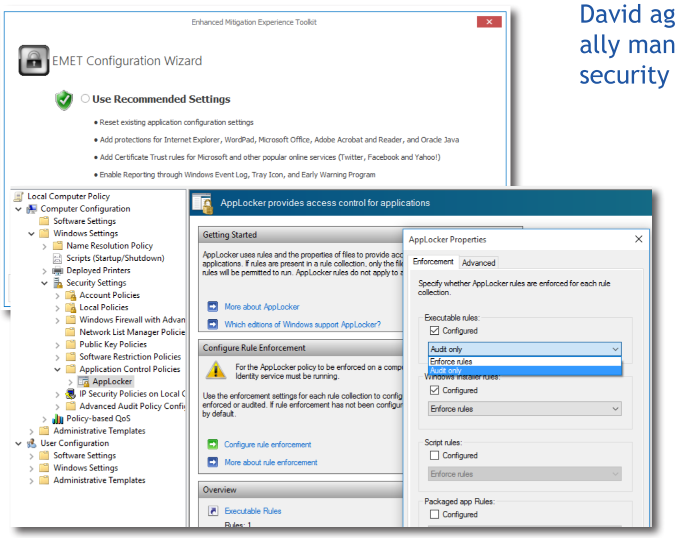


Figure 6: Thales' survey reflects the findings of the Verizon report which concludes that 80% of breaches originate from external sources

Adam again: "Most struggle to identify what the sensitive data is, where it is, and where it goes, whereas working with perimeter security is a relatively known quantity"

David agreed with this, adding "It's easier, better understood, and usually manageable in-house. Network security is easier than end-system security and the skill-sets more prevalent"



Enhanced Mitigation Experience Toolkit

EMET Configuration Wizard

○ **Use Recommended Settings**

- Reset existing application configuration settings
- Add protections for Internet Explorer, WordPad, Microsoft Office, Adobe Acrobat and Reader, and Oracle Java
- Add Certificate Trust rules for Microsoft and other popular online services (Twitter, Facebook and Yahoo!)
- Enable Reporting through Windows Event Log, Tray Icon, and Early Warning Program

AppLocker provides access control for applications

Getting Started

AppLocker uses rules and the properties of files to provide acc
applications. If rules are present in a rule collection, only the fil
rules will be permitted to run. AppLocker rules do not apply to a

More about AppLocker
Which editions of Windows support AppLocker?

Configure Rule Enforcement

For the AppLocker policy to be enforced on a comp
Identity service must be running.

Use the enforcement settings for each rule collection to config
enforced or audited. If rule enforcement has not been configur
by default.

Configure rule enforcement
More about rule enforcement

Overview

Executable Rules
Rules: 1

AppLocker Properties

Enforcement | Advanced

Specify whether AppLocker rules are enforced for each rule collection.

Executable rules:
☑ Configured
Audit only (Enforce rules / Audit only)

Windows Installer rules:
☑ Configured
Enforce rules

Script rules:
☐ Configured
Enforce rules

Packaged app Rules:
☐ Configured

Mark at NNT: "The Verizon data referenced earlier does back this up. Their figures will tell you that over 80% of attacks originate from external sources.

So whilst it makes sense to focus on perimeter defences it also misses the point - ultimately the servers and desktops holding the data need to be protected. Buy extra bolts for your front door, sure, but get a safe for your valuables as urgently.

My issue is that most organizations would get a big boost in security simply by taking time to not just harden in line with CIS guidance, but also implement the built-in security defences they already own.

For example, anyone with Windows 7 onwards will have access to EMET – phenomenal security for applications on the desktop and server and just needs to be installed and enabled, likewise User Account Controls and MS AppLocker provide policy-based application operation, and you might even check out BitLocker for encryption. Layered Security is still the goal - better to have overlapping measures than gaps".

WHAT IS THE LATEST GUIDANCE WITH RESPECT TO RANSOMWARE?

HOLLYWOOD PRESBYTERIAN MEDICAL CENTER
HOLLYWOOD PRESBYTERIAN MEDICAL CENTER

Figure 7: Dangerous Precedent? *The Hollywood Presbyterian Med Center paid a $17,000 ransom when hit with a Cyber Attack*

Ransomware is proving to be lucrative for cybercriminals and, like the Great White Shark, you never know when it will strike. But when it does, its going to hurt!

- The Great White Shark of Malware – the most feared malware there is
- Typical ransomware demands range from $300 to $600
- What value would you place on all your photos, music, documents?
- For a corporation, the LA Presbyterian Hospital paid the equivalent of $17,000, setting a dangerous precedent (and now, Methodist Hospital in Kentucky, is also reported to have been targeted)

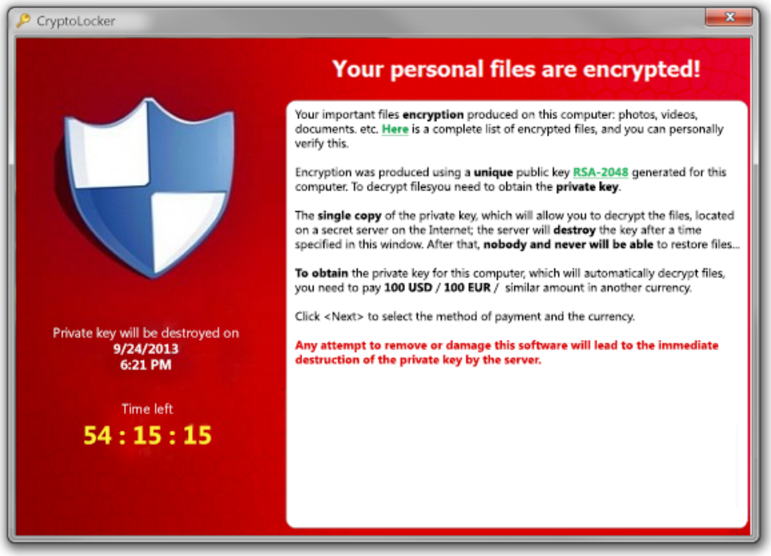
What is the latest guidance from the panel regarding the Ransomware threat, how we should be defending against it and what we should do if we do get hit?

Adam grabbed this question too: “Follow the advice in frameworks like the CIS Controls which will have you doing things like whitelisting, training folks to see phishing attempts, and having good backups at the ready. Ransomware is not a dramatically new attack, just a monetized one”

Mark Kedgley: “We’re back to the earlier question of Perimeter vs Endpoint. Ransomware targets the desktop through phishing emails with toxic web-links or malicious attachments.

The majority of exploitable vulnerabilities can be mitigated within the Workstation Operating System, and further protection can be provided using manufacturer extensions such as Microsoft’s EMET (Enhanced Mitigation Experience Toolkit) and Windows Defender or 3rd Party AV.

The ***NNT Ransomware Mitigation Kits*** first audit the desktop applications for vulnerabilities, then automatically harden the browser, office apps and email”



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

***Figure 8**: **You don’t want to see this** Classic Ransomware operation - after the malware is in place, a unique encryption key is generated for each computer infected and is used to encrypt data on the machine. If the ransom is not paid within the allotted time the files are lost forever. Make sure backups are up to date and isolated from the computer, otherwise they may be encrypted too.*

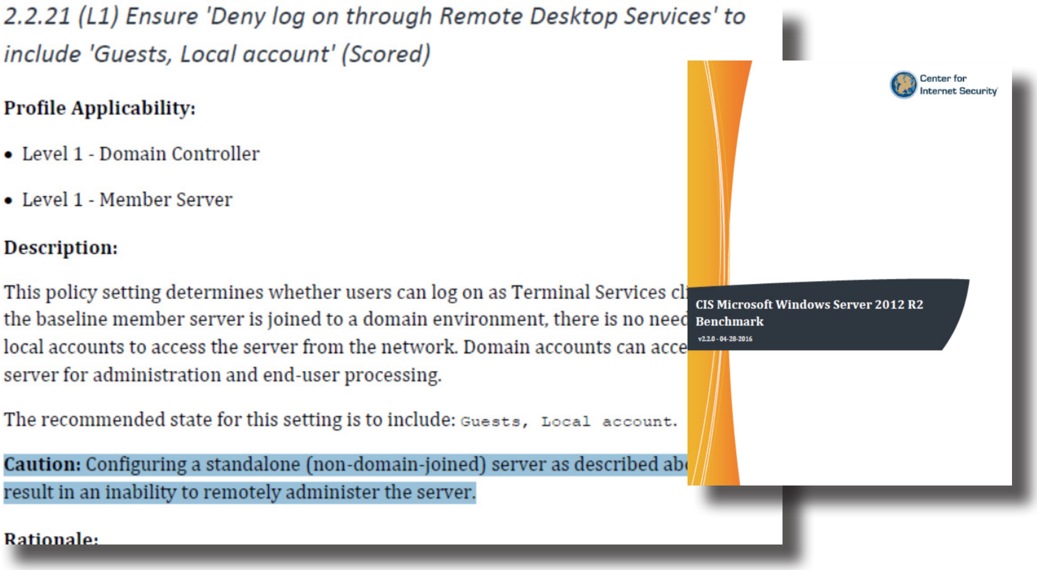
ELIMINATING VULNERABILITIES BY HARDENING COMES WITH A HEALTH WARNING - WHAT IS THE SAFEST WAY TO DO IT?

The most secure server is one that is disconnected from the network then powered off – and also not much use in running applications. So there is a balance to be struck.

What is the best route to getting the maximum protection without damaging service delivery?

***Figure 9: Caution!** Hardening a system involves removing features and function that is known to render the device vulnerable to attack.*

Often this same functionality has the potential for legitimate, useful usage - so decisions need to be made at each step, especially as complex application operation and interaction may depend on config settings that aren't at all obvious.



2.2.21 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can log on as Terminal Services cl the baseline member server is joined to a domain environment, there is no need local accounts to access the server from the network. Domain accounts can acce server for administration and end-user processing.

The recommended state for this setting is to include: `Guests, Local account.`

Caution: Configuring a standalone (non-domain-joined) server as described ab result in an inability to remotely administer the server.

Rationale:

Center for Internet Security

CIS Microsoft Windows Server 2012 R2 Benchmark

v2.2.0 - 04-28-2016

***Figure 9:** Sample from a CIS Benchmark, the industry's recognized standard for secure configuration guidance*

Mark and David had a strong consensus on this: "There are three cooperative ways to mitigate this risk: Simplify, provide advanced information, and test.

Provide security requirements to your development team as early as possible. Better yet, have security personnel contributing to every development team. There needs to be as much early-stage consideration to security planning as there is to the sizing of hardware and network design"

Adam concurred: "Establish a test environment that is as close to production as possible and then include rolling changes to that test environment before rolling them into production.

Regarding our CIS Benchmarks, they usually preface any 'risky' measure with a Caution note as in the example above.

Generally speaking, these are the steps you really need to think hard about as to whether these may be a step too far. At the same time, the more hardened the better, you just need to think about your own situation and how you choose to balance security and ease of use.

Of course, once you have a hardened config you then need to keep it that way - we talk about the need for a 'rigorous config management and change control process' in the CIS Secure Controls".

FINALLY, WHAT ARE THE TEAMS' TAKEAWAY TIPS FOR IMPROVING CYBERSECURITY?

Adam from CIS: "Get informed: Use resources like the learn.cisecurity.org website that provides free to use CIS Benchmark content"

David from Core Concept: "Beware buying security products too early and before you have properly understood what you are trying to secure, so make sure you get help. My pet phrase as a South African is 'Build your fence higher than your neighbors' - Cyber attackers are lazy and will attack the easiest targets so make sure you are doing the basics well"

Mark from NNT: "As mentioned earlier, use the untapped security measures you have at hand: implement CIS hardening measures - of course! - but make sure you leverage freely available extras such as Microsoft EMET, AppLocker and BitLocker which provide valuable added protection.

With so much ground to cover and security best practices to implement, use automation to assess vulnerabilities and to remediate them."

ABOUT THE CENTER FOR INTERNET SECURITY AND NNT

The Center for Internet Security is the primary recognized industry-standard for secure configuration guidance, developing comprehensive, consensus-derived checklists to help identify and mitigate known security vulnerabilities across a wide range of platforms.

Each CIS Benchmark provides prescriptive guidance for establishing a secure configuration posture for your IT Infrastructure, including a detailed description and rationale of potential vulnerabilities together with clear auditing and remediation steps. As such, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leech Bliley and ITIL.

NIST 800-53 SP
Sarbanes-Oxley (SOX)
NERC CIP
FDCC US Government Secure Configuration Baseline
State of California Data Security Breach Reporting
CIS SECURITY BENCHMARKS CERTIFIED
ISO 27001/27K
FedRAMP
PCI DSS V3.2
HIPAA HITECH
DISA STIG
CESG Assured Service (Telecoms) - CAS (T)
CYBERSECURITY 500
WORLD'S HOTTEST SECURITY COMPANIES

As part of the CIS community, NNT has access to consensus security configuration benchmarks, software, metrics, and discussion forums where NNT is an integral stakeholder in collaborating on security best practices. NNT has leveraged these resources and best practices in our products to measure and improve the security posture of our customers. As of May 2014, NNT Change Tracker has been awarded CIS Security Software Certification for CIS Security Benchmarks across all Linux and Windows platforms, Unix and Database Systems, Applications and Web Servers.

Note: NNT is also an Official OVAL Adopter and can equally utilize any 3rd party source of SCAP, OVAL or XCCDF content, for example DISA STIG checklists.

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combin-ing: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative. W: www.newnettechnologies.com E: info@nntws.com