Change is the Enemy of Security:

Ten Network Changes That You Should Be Looking For

By David Meltzer

INTRODUCTION

Your network is evolving.

New assets are joining your network. Users are installing new applications. Network services are opening and closing. File permissions are changing. An application vendor is about to issue a patch. Somewhere, a bored teenager is designing a new virus. A valued IT employee is thinking about leaving the company.

The average enterprise network experiences thousands of changes per day. And many of these changes chip away at your security posture, causing your network to drift away from its most secure state.

Any one of these changes could be the one that introduces a major security risk.

Unfortunately, you can't stop time and you can't stop change. Managing this torrent of change must become part of your operational security plan or your security posture will inevitably fall prey to the forces of time.

So how do you do this?

By moving away from "snapshot security" and monitoring your network for changes continuously, you can analyze the changes the minute they happen, logging the benign changes (for audit and compliance purposes) and fixing the dangerous ones (for security purposes). Fixing a small problem is faster and easier than fixing a big one. And by monitoring for and reacting to change immediately, you find and fix problems while they're still small.

Here are ten ways that enterprise environments typically change, all of which can chip away at your security in ways that you might not realize. Some are obvious; some are subtle; all could be dangerous.

1. AN UNAUTHORIZED DEVICE JOINS YOUR NETWORK

Any device attached to your network without authorization is a rogue device. Since these devices fall outside official network inventories, legacy agent-based asset management systems are unaware of their existence, and traditional security tools have no way to discover them amongst the sea of legitimate assets.

A common example of a rogue device is an unapproved, unsecured wireless access point and anything that attaches to it. However, many other sources of rogue devices place corporate assets at risk, such as:

- Laptops brought in by consultants and visitors
- Home machines brought in by employees
- Employees connecting PCs or home networks to the corporate LAN via VPN

In addition, any device that lacks the controls in place to keep it updated and in compliance with security policy can reasonably be considered as rogue. Since such a device lies outside the direct control of security administrators, you must consider it a threat.

The average enterprise network experiences thousands of changes per day. And many of these changes chip away at your security posture, causing your network to drift away from its most secure state.

The Risk

Rogue devices can be serious vectors of infection. Since they lie outside the purview of security control, you usually have no knowledge about their configuration, their security status, or the intent of their operators. The presence of rogue devices on a network is usually a serious violation of regulatory standards.

What should you do when an unauthorized device joins the network?

Discover: Monitor your network continuously for devices joining the network so that you can detect newly-active devices immediately. Conduct a detailed inventory of each new asset to determine its configuration and state.

Analyze: Perform a security analysis against the new asset to determine if it is in compliance with security policy and if it poses any serious risk.

Act: If the asset poses a serious and imminent threat to security posture, it should be quarantined or blocked from access to the network. Less critical threats should be identified by an administrator and assigned an appropriate asset owner within the IT organization who is responsible for ensuring the system is remediated to comply with security policy. All such asset appearances should be recorded for audit and forensics purposes.

2. MOBILE SYSTEMS JOIN AND LEAVE YOUR NETWORK CONTINUOUSLY

Mobile systems such as laptops, personal digital assistants (PDAs) and smart phones present their own distinctive challenges. The same features that support easy and immediate communications at airport and coffee shop hotspots also leave these tools open to compromise.

The Risk

This risk expands exponentially every time a mobile device reconnects to your corporate network. If the laptop was outside your control and potentially networked with anyone, anywhere, it may or may not have been compromised. You have no way to know until it reconnects to the network—as a trusted device inside the network perimeter.

On top of this, it is extremely difficult to enforce a security policy when IT security has intermittent access to the target device. Mobile systems pose significant risks to security compliance initiatives.

Mobile systems such as laptops, personal digital assistants (PDAs) and smart phones present their own distinctive challenges. The same features that support easy and immediate communications at airport and coffee shop hotspots also leave these tools open to compromise.

What should you do when a mobile system joins the network?

Discover: Monitor your network continuously for mobile systems joining the network. Ensure that you are able to identify systems even though they may be connecting with different IP addresses and on different parts of the network.

Analyze: Perform a security analysis against the new asset to determine if it is compliant with security policy and if it poses any serious risk.

Act: The major difference between mobile assets and rogue devices is that mobile assets are known to IT. There should exist a process for monitoring and updating mobile assets.

If the mobile asset poses a serious and imminent threat to security posture, it should be quarantined or blocked from access to the network. Less critical threats should be identified by an administrator and assigned an appropriate asset owner within the IT organization who is responsible for ensuring the system is remediated to comply with security policy. All such asset appearances should be recorded for audit and forensics purposes.

3. NETWORK ASSETS DISAPPEAR FROM YOUR INVENTORY DATABASES

Over time, your devices often become misplaced. They remain connected to the network, but there is no record of their location.

If there's no change in their function, you are unlikely to find them, even with network behavior monitors.

Assets usually become "stranded" (as they are now called) for any number of valid reasons: Sometimes an act as simple as an agent crashing or getting inadvertently removed can cause an asset to be lost. In other cases, a merger or reorganization may occur and nobody really knows what assets were there to begin with…

This is not something you notice unless you're looking for it, but it has happened in 100% of the companies that Cambia has talked to and usually involves 2-3% of the total network asset base. However, the industry analyst RHK, Inc. estimated in 2002 that as much as 20% to 30% of telecommunications industry network assets become stranded over time. Even a fraction of this amount represents a serious threat to network security and performance.

The Risk

Stranded assets are not actively managed or updated. They become prey to common compromises and are often the primary access method for further incursions into a network. In addition, stranded assets represent a significant violation of many regulatory standards.

What should you do to prevent network assets disappearing from inventory databases?

Discover: Regularly monitor your network asset base using a combination of active and passive network discovery monitoring. Continuous monitoring is optimal. Ensure that your network monitoring can uniquely identify systems whose IP address, system name, and location may change over time, and will find network-connected assets regardless of the software running or configuration state.

Also ensure that you capture as much information as possible about asset configuration, including asset type, OS, installed applications, patch levels, and configuration settings. You will use the detailed information to identify stranded assets.

Analyze: Compare the results of your network monitoring with your inventory database. Identify unmanaged systems by finding systems that are out of compliance with policy, out of date, lack typical software packages or contain unusual software, or that have not been "touched" for longer than comparable systems.

Act: (Re-)Populate your inventory database using the results of network monitoring. Schedule remediation for any systems that are out of compliance and assign an owner to each.

4. A NEW PATCH IS AVAILABLE FROM A TECHNOLOGY VENDOR

Service packs, hot fixes and patches for operating systems and applications provide critical pathways for closing security exposures before vulnerabilities lead to attack. And yet, tracking the exponential growth in patches for nearly every hardware or software product deployed in a typical enterprise environment is an overwhelming task. Actually implementing all these in-service repairs in a timely manner is all but impossible.

Poorly planned patching efforts can lead to serious service interruptions—or even rejected remediation efforts if your network security solution itself sees the patch as a threat. You need real-time insight into which systems have been upgraded to any given patch level, including clear prioritization criteria so that the most critical systems are upgraded first. And yet, it is exactly this information that you are most likely to lack.

The Risk

Patches aren't always applied correctly, even when a patch management system says they are. Lack of patches represents a significant security risk, particularly when you believe they've been applied successfully.

Cambia is aware of one situation in which the patch management system successfully loaded a patch file onto a set of critical servers, but each server's local Cisco Security Agent treated the patch files as an intrusion and prevented them from being installed.

Each security product was performing its function properly, but the overall security posture was not improved.

What should you do when a new patch becomes available?

Discover: Use your asset inventory database to identify all the systems in your asset database that *should* have the patch installed.

Analyze: Configure internal security policy to require the new patch level. Use the asset configuration monitoring system to identify any non-compliant assets. Compare the list of non-compliant systems with the list of systems patched.

Act: Use your patch management system to apply the patch. Then, use a third-party (i.e., non-patch-management) system to validate that patches have been applied successfully. Ensure that this system can identify operating systems, applications, and patch levels.

5. NETWORK-AWARE APPLICATIONS ARE INSTALLED ON YOUR NETWORK

The software counterpart to a rogue device is an unauthorized application. Any code that executes on your network without your explicit approval and supervision has the potential to carry a malicious payload. Peer-to-peer applications, instant messaging, guerilla Web or FTP servers grab the most attention, but any installer that comes from an untrustworthy source places corporate assets at risk. Hundreds or thousands of users on an enterprise network represent endless opportunities for unauthorized applications to be installed, which greatly complicates your ability to remain on top of this challenge.

The Risk

Software applications themselves may inadvertently disguise malicious or unauthorized traffic. Encrypted programs such as SSH, remote control applications and desktop redirectors that route corporate email to PDAs and smart phones all create traffic that, even when legitimate, cannot be "read" by firewalls, antivirus or most intrusion detection/protection systems. If you cannot recognize these unauthorized services when they first connect to your network, you cannot stop attacks that use these tunnels until after they have penetrated the network perimeter.

What should you do when a new network-aware application appears on your network?

Discover: The most important aspect of your security policy in this regard is the ability to discover new network services quickly. Continuous network monitoring with active and passive scanning capabilities usually gives you the best combination of timely detection and detailed information.

Analyze: When you detect a new network service, immediately analyze it for security risks using a signature-based vulnerability scanner.

Act: If the new application represents significant security risk, you should attempt to quarantine the affected device immediately by disabling network access or altering firewall settings. You should also notify the appropriate administrator(s) immediately and attempt to roll back, patch, or otherwise remedy the security risks. Often the solution for remedying the problem of new applications is to remove the application from the network entirely, and not to simply patch the application, which would have the effect of leaving your network with a secure, yet still undesirable, application on your network.

6. YOUR USERS DON'T FOLLOW SECURITY POLICY

Systems and devices can be in perfect alignment with security policy, but still carry serious configuration errors. For example, inappropriate file permissions, weak passwords or passwords written down and left in plain sight all represent threats that cannot be uncovered through traditional discovery processes.

The Risk

A 2003 Gartner report estimates that 65% of cyber attacks come from system configuration errors—and only 35% result from software vulnerabilities.

What should you do to enforce sound security practices?

Discover: Even though this is an issue with user behavior, it can be detected with a security solution that has sufficient access to user assets. A system needs to be in place that can discover detailed asset configuration information and continuously detect changes to those configurations. Security policies, when translated to actual system configuration, often consist of hundreds of settings and objects. Your asset configuration monitoring system needs to be able to handle this level of detail and continuously audit your assets for compliance with internal policy.

A combination of passive and active network scanning techniques can discover and log asset configurations in detail.

Analyze: Compare discovered asset configuration with internal security policy. Determine not only what assets are out of compliance, but to what degree, and what risk the non-compliant state poses. Continuous discovery and analysis will catch non-compliant changes as they are made.

Act: Notify users and their managers about non-compliance. Create a culture where adherence to security policy is valued and rewarded and non-adherence is penalized. Some IT administrators may even choose to quarantine non-compliant systems or rollback unauthorized changes.

7. ACCESS PERMISSIONS CHANGE FOR A KEY ASSET

Two colleagues in accounting need to share some data files relating to an upcoming earnings report. They know their systems are networked and on the same segment. So one changes the file access permissions so that his colleague can now read and modify the necessary files.

Unfortunately, so can the rest of the company.

Dozens of small, seemingly innocuous changes like this cause an asset's configuration to drift, exposing more and more sensitive data to unauthorized access. Many companies don't regularly look for security breaches like this one.

The Risk

Putting aside the issue of regulatory compliance, this example is perhaps the most effective illustration of how change is the enemy of security.

Multiply this small change by thousands per day and it becomes clear how serious security risk can gradually emerge, not from one big change, but from a thousand small ones.

What should you do to prevent dangerous changes to access permissions?

Discover: You must continually monitor your network for change. "Snapshot security" might catch this type of risk, but only after it's been active for a while.

Analyze: Upon detecting a change, you must analyze it for security risk. This requires that you understand which assets contain valuable information.

Act: Fix any problems you find immediately. It's easier, faster, and less costly to fix a problem when it's small and new than when it's been around for a while. In this particular example, the broad file share permissions should be detected the instant the change is made and rolled back immediately, with notification to the user making the change that such a change is dangerous, unauthorized, and non-compliant.

8. YOUR NETWORK DEVELOPS A LEAK

Data files are the most shared resource on your network. After all, how useful would email be without the ability to send a spreadsheet or document for someone else's comments and edits? Most end users know that the most straight-forward means to move files from system to system is to create a shared folder on a Windows system, or set up a centralized server via NFS or a network attached storage (NAS) device.

The Risk

The challenge with shared resources is that the file being shared easily passes beyond the control of the security infrastructure. A spreadsheet comes home on a laptop, and then gets transferred to a home PC for work over the weekend. Once there, it can easily become infected with a worm or virus prior to transport back inside the network perimeter. Anyone who then accesses that file risks introducing a full-fledged outbreak inside the corporation.

In addition, many organizations use open file shares for posting public information across the enterprise. These resources are often abused for "temporary" storage, with inadequate examination of the files' contents—including the inadvertent disclosure of confidential information. Many groupware, database or Web applications rely on file shares to distribute content or create a collaborative work environment. Any misconfiguration of user privilege risks opening this information to broad distribution, while still appearing as if the application is functioning as intended.

What should you do to prevent a network leak?

Discover: Monitor your network continuously for change, where "change" involves the appearance of existing assets from new locations and changes to file permissions. You should also consider monitoring outgoing communications for sensitive data.

Analyze: Establish a security policy that prohibits chained network shares that transcend your network boundaries. Prevent open file shares.

Act: Notify users and administrators when monitoring detects unsafe chained network shares and close them immediately. Open file shares should also be closed.

9. A LEGACY SYSTEM "GURU" LEAVES THE COMPANY

Every organization has special-purpose devices, such as a plotter that requires OS/2, legacy applications running on an AS/400 or an IRIX server placed in production years ago but still perfectly functional. As the original support staff for these devices leaves the company or move on to other responsibilities—and as technical assistance becomes unavailable from the manufacturer—the means and knowledge to secure these devices become increasingly rare.

The Risk

You cannot be the expert for all these one-off systems, and yet they must either be protected or identified and retired.

What should you do when a guru leaves?

Discover: Monitor the affected systems continuously for suspicious activity and changes that could create risk. Commercial products to analyze these systems for change may be difficult or expensive to obtain, but you may be able to obtain useful information from standard active network scanning and passive monitoring of network traffic.

In some cases, you may wish to identify a few critical objects to monitor for change and develop a custom check to watch those objects. For example, an older UNIX variant may have an SSH interface to it through which you can enumerate users and software packages running with 2 simple commands. Use a system where you could add these 2 custom checks into your enterprise change monitoring and you will now have controls in place to protect these from becoming stranded in the future.

Analyze: Decide whether or not it still makes economic sense to continue using the legacy product, given the increasing support costs. If you decide to continue using the assets, make a small investment in change monitoring for the assets upfront so that the system will be maintained in a secure state down the road.

Act: If so, you'll need to assign and train personnel to secure the affected systems. You may also want to quarantine legacy systems behind internal firewalls with very strict access controls.

10. YOU INSTALL NEW SECURITY HARDWARE OR SOFTWARE SYSTEMS

Over the last few years, network security infrastructure has become increasingly capable and considerably simpler to deploy and manage. You trust these devices implicitly once the initial configuration and hardening process is complete.

The Risk

Unfortunately, security infrastructure is just as prone to misconfiguration, inappropriate and/or outdated policy, or hardware failure as any other group of devices. Plus, the configuration of your security systems needs to keep pace with the other changes happening on your network.

What should you do when new security systems are installed?

Discover: Hopefully, you're already monitoring the rest of your network continuously for change. Your monitoring should also include your security products. Any changes to firewalls, IDS/IPS systems, anti-virus systems, etc. should be noted and logged. Where security

products reside on assets outside the control of IT, pay particular attention to users' tendencies to disable or weaken protections.

Analyze: Your security policy should explicitly state who is permitted to alter the configuration of a security product. Unauthorized access to security systems is, needless to say, a significant security risk.

More importantly, you also need to analyze the configuration of your security systems to ensure that they are adequately enforcing your security policy, as that policy inevitably changes. Many security products require frequent, even daily updates, to properly protect a system. You should have processes in place to identify what systems need to be updated and make sure updates are being monitored and tracked as part of your policy (this might need to be split into discover as well).

Act: Most actions relate to configuration changes for protected assets. However, as you make security monitoring an on-going process, be sure to include your security systems in your remediation plan as well. Update firewall rule sets, IDS/IPS configurations, and anti-virus settings to track the changes in your network.

CAMBIA CM—AUTOMATED DETECTION & SECURITY ANALYSIS OF ALL NETWORK CHANGES

Cambia CM is a network-based security and change management application that automates detection and impact analysis when any device or application on a network is installed, removed, or altered in any way. Cambia CM provides constant, non-intrusive monitoring across networks and devices. Any change is immediately and automatically ranked according to relative risk and urgency, and escalated to the appropriate staff for remediation.

Cambia CM brings rogue devices and applications, unpatched applications and operating systems, or any other security exposure not covered by traditional security infrastructure into a highly structured, real-time change management framework. As a result, Cambia CM helps security administrators:

- Document gaps in the security infrastructure
- Demonstrate how they came about
- Communicate how to repair the exposures and prevent their recurrence
- Gain the resources and management support necessary to proactively prevent attack and misuse

Cambia CM's continuous network surveillance harvests network intelligence that significantly improves the performance of existing network security infrastructure. Customers using Cambia CM's change management security model achieve significantly improved network protection with excellent, rapid return on investment.

Cambia CM also provides the audit and reporting structure necessary to document security concerns and the steps taken to resolve them—including documentation necessary to support regulatory compliance efforts. In short, Cambia CM automates three essential steps for managing change across enterprise networks:

1. Establish real-time visibility into any change on the network.
2. Rapidly analyze changes and prioritize them according to severity, then correlate the likelihood of attack to the value of the asset at risk.
3. Develop a remediation plan that fixes critical exposures fast, with open communication with management so that risks and implications are well understood, and the patch process fully funded and supported.

NaSPA member David Meltzer founded Cambia Security, Inc. in January 2003 to bring his vision of using change detection to enhance security operations into reality. He is an IDS pioneer, an original author and the lead developer of the market-leading RealSecure IDS from Internet Security Systems.

Mr. Meltzer is also a respected researcher, discovering numerous vulnerabilities and co-founding ISS's X-Force security research group. Immediately prior to Cambia, David was the founder and CTO of Sonicity, a secure multicasting software company whose technology was acquired by Sony in November 2001. Mr. Meltzer has a B.S. in Computer Science from Carnegie Mellon University.