

How to Shore Up the Weakest Points in Your Network: People



Numerous forensic studies of serious data breaches show that human errors often were 'causal events' leading to the breaches. Allied Telesis addresses the weak points where human failures lead to vulnerabilities.

Introduction

There's a persistent message coming from cybersecurity vendors – "Protect your network borders, don't let the bad guys in!" While this is a prudent strategy, it is not the only strategy a modern organization needs to have to protect its network. We see examples every week of network breaches, data theft and cyber-crime affecting organizations of all sizes, across all industries.

The reality is, network breaches and business disruption will happen because threats do not only come from malicious sources but also manifest themselves as accidental configuration errors by trusted network admins, and from employees following poor work practices. Both can lead to network outages that disrupt business or vulnerabilities that can be exploited by bad actors.

According to the 2018 Cost of a Data Breach Study, around 25% of all U.S. data breaches were recognized as carelessness or user error.¹ It's time that companies realize that once they have adopted conventional network security measures, their biggest vulnerability is their people.

Even the largest organizations with huge resources struggle to protect themselves from these "weak points." In July 2019, Capital One Financial Corp.

revealed it had a major breach affecting 106 million people in North America. Forensic analysis traced the breach back to a configuration vulnerability that enabled a cyber-thief to download 30 GB of sensitive financial information.² If a large financial services company like Capital One can't get it right, what can be expected of everyone else? The answer is that companies need to assume that a security breach will occur and adopt a variety of strategies to plan for it.

“

*25% of all U.S. data breaches were recognized as carelessness or user error...
77% of organizations do not have a cybersecurity response plan.*

”

Let's look at two types of weaknesses organizations typically have and how to overcome them:

- **Configuration errors** – According to the 2018 Verizon Data Breach Investigations Report, 17% of data breaches were caused by mistakes.³
- **Insider threats** – That same Verizon report indicated that 20% of data breaches were caused by insider threats.⁴

Configuration Errors

Configuration errors have been around forever and like software bugs, are notoriously hard to prevent. More than a third (37%) of service incidents are due to configuration or other human error and could be avoided with proper monitoring, configuration management and automation.⁵ The reason for so many mistakes is simple—network devices are configured using esoteric commands that are complex and easy to get wrong. Worse, a network device cannot always detect that the wrong command has been entered, so some errors can lie undetected, causing mysterious outages or subtle vulnerabilities that others can exploit.

“

in June 2019 the Google Cloud network... outage was pinned on a server configuration change that was... incorrectly applied... leading to the massive outage.

”

Unfortunately, there is no easy remedy and such errors remain an important issue to try to address, as they can have serious ramifications. For example, in June 2019 the Google Cloud network had an outage lasting four hours that affected Google’s own services, including YouTube, Gmail, Google Search, G Suite, Google Drive, Nest, and Google Docs, as well as numerous customers who host their applications on Google Cloud. The root cause of the outage was pinned on a server configuration change that was intended for a small number of servers in a specific region. However, the configuration was incorrectly applied to a larger number of servers across several neighboring regions, and it caused those regions to stop using more than half of their available network capacity, leading to the massive outage.⁶

New Intent-Based Networking tools should help as they minimize the need for complex commands using graphical tools and natural language instead. However, these tools are expensive and require network upgrades. Some doubt their effectiveness, so adoption is not yet widespread, especially in smaller organizations. Therefore, configuration errors will likely continue to be a source of internal threat for some time to come.

Another approach that has made a tangible improvement is the use of automation to help reduce the amount of manual configuration required. Automation tools typically rely on the administrator to create scripts that can be executed on multiple devices to reduce the risk of mistakes. Of course, if the script is wrong then there’s a chance the error will be propagated across multiple devices, but the use of sandboxes and test environments can help mitigate that risk.

Alongside this automation approach, Allied Telesis offers an additional ability to allow the admin to use the command line as normal, but to dynamically replicate any commands to multiple devices to reduce the chance of mistakes creeping in from one device to another—a common source of configuration errors. This approach works well when the commands specify a common configuration on many devices (like adding a VLAN or ACL). Instead of typing the commands several times, the admin only need enter them once and the tool will ensure they are faithfully copied to the other devices. In this way, we reduce the chance of errors being created, rather than try to identify them afterwards with testing and verification, which is time-consuming and not always successful.

Insider Threats

It’s incredibly difficult to build a network that has a 100% secure border. Almost all networks have weaknesses and often the people that use the network offer the greatest risk. Yet very few companies adequately train their staff with the skills to identify and avoid these threats. MediaPro’s State of Privacy and Security Awareness report claims that 70% of US employees don’t understand cybersecurity.⁷

“

70% of US employees don’t understand cybersecurity... 65% of insider incidents are related to accidental mistakes or misuse.

”

Sometimes breaches are deliberate and malicious, where an employee abuses their trust and causes damage, steals or enables others to steal from the company. Restricting access to sensitive data, data leak prevention, network segmentation, enforced policies and procedures, and audit trails are effective ways to limit this exposure. Although insider threats are less common than external threats, the damage can be much worse and a motivated person with malicious intent and access to company data can be difficult to stop.

One of the most famous and damaging insider breaches of all time was when the contract employee Edward Snowden stole classified information from the National Security Agency (NSA) and exposed it to journalists. If one of the most security-conscious agencies on the planet can't safeguard its most sensitive secrets from insider threats, what organization can?

A more common threat is the inadvertent mistake from an employee who "just forgot" or "didn't think" when they introduced a threat. The Ponemon Institute says that 65% of insider incidents are related to accidental mistakes or misuse.⁸ Common mistakes are the use of unknown USB sticks, sharing passwords (yes, it still happens), storing sensitive information on unsecured devices then losing them, connecting unauthorized devices to the company network, falling prey to phishing campaigns, forgetting to apply a security patch, etc. Each of these mishaps has the potential to expose the organization to threats that may lead to business disruption, reputational damage, significant fines and other financial outlays.

We'll look here at the class of mistakes that enable threats to enter the network by a backdoor or an alternate route other than the usual email or weaponized website. This is especially troubling because most networks rely on their firewall to protect them from threats—the "secure border" model. If threats can bypass the border (just as the Greeks entered Troy inside the famous wooden horse!) then the network is defenseless against them and threats can spread and wreak havoc with nothing to stop them.

Worse still, the administrator might become aware of the issue because his firewall starts reporting that it sees a threat, but what can he do about it apart

from pulling network cables out? Some threats spread too fast for a human to catch. Hence the traditional approach is to defend the border at all costs and keep the threats out—the reason being that once the attackers get inside, as the Trojans discovered, it doesn't end well.

A better approach is to apply another strategy; one that accepts that threats can and will enter the network and offers solutions for how to deal with them effectively and quickly. Ideally, the network would not only identify the threat, but it would take immediate action to shut it down and isolate any affected devices before it could cause more damage. This is exactly what the Self-Defending Network solution from Allied Telesis does.

Working with the existing firewall, so no replacement or reconfiguration is required, the Self-Defending Network can react whenever the firewall sees a threat to identify the source of the threat and isolate the affected user device. Other solutions exist that do the same thing but they all require agent software to be loaded onto the endpoint

“

Ideally, the network would not only identify the threat, but it would take immediate action to shut it down.

”

devices so they can be controlled. This limits the solutions' effectiveness and complicates deployment of new devices, adding to the administrator's busy workload.

The Self-Defending Network is different because we control the network, not the device—so there is no agent software to deploy and we can protect against threats on any user device. Also, we can protect both wired and wireless networks since we can isolate wireless devices too. However, the greatest benefit of the Self-Defending Network is that the responses to threats are automatic and immediate, so no manual intervention is required to shut down a threat and it has no chance to spread. This solves the problem of how to stop a threat from escalating once it gets beyond the border's defenses. As an automated solution, it even helps

prevent human errors when fighting an internal threat, when time is short and stress levels are high.

A Deeper Dive - Allied Telesis Solutions to Overcome Vulnerabilities

The sections above have laid out the case that people are often responsible for the weak points in a networked environment, whether it's intentional or accidental. Allied Telesis has developed innovative technology-based solutions to address these specific areas—to reduce configuration mistakes, and to automatically defend against threats that skirt the enterprise firewall. Let's take a deeper dive on each of these solutions.

The Autonomous Management Framework Plus (AMF Plus)

Allied Telesis' Autonomous Management Framework Plus (AMF Plus) tames the challenges of the manual configuration process that so often lead to mistakes. AMF is a scalable network management platform that supports Allied Telesis switching, firewall and wireless products, as well as a wide range of third-party devices for truly inclusive network automation.

AMF Plus reduces the time and skill required to maintain the network. Powerful features like centralized management, auto-backup, auto-upgrade, auto-provisioning, and auto-recovery enable plug-and-play networking and zero-touch management.

“

Configuration changes that might ordinarily take hours can be done in minutes through automation.

”

As for configuration changes, they can be made on multiple devices simultaneously. Commands are issued only once and AMF Plus ensures that

they are received and processed by each device designated for the change. This saves time and reduces the chance of mistakes when configuration changes need to be made across multiple devices. Any configuration change, monitoring request or debugging of the network can be made to one, many, or all devices with a single command. Configuration changes that might ordinarily take hours can be done in minutes through automation.

AMF Plus auto-backup reduces effort and the risk of errors by automatically managing the configurations for all devices in the network. Every day, AMF Plus automatically backs up the configuration and firmware for the entire network into a central library. Backups also can be created manually after configuration changes. Up-to-date firmware and configuration information is always available for all devices so that failed devices can be automatically regenerated.

Firmware upgrades can be rolled out to groups of devices or the entire AMF Plus network quickly and easily with auto-upgrade. The admin simply selects the group of devices to be upgraded, then issues the CLI commands to load the new firmware release. Each device in the group will download the files in preparation for a reboot. AMF Plus can use a rolling reboot process to ensure that only one device at a time is offline in order to maintain maximum network connectivity.

Auto-provisioning allows unconfigured devices to be added directly into the network because AMF Plus can pre-provision the device even before it is present. This allows zero-touch expansion of the network, as devices can be easily added and AMF Plus automatically selects the correct configuration. If a new device hasn't been pre-provisioned, then AMF Plus isolates the device until it has been successfully configured, either automatically by AMF Plus or manually by the admin.

These various capabilities of the Autonomous Management Framework Plus not only save time and money but also, importantly, reduce the likelihood of configuration mistakes that can be so damaging to a network.

The Self-Defending Network



AMF-Sec can isolate compromised endpoints devices without the need to install agent software.



AMF Plus also can be used to create a self-defending network using software called the AMF Security Controller. AMF-Sec is an innovative solution that can monitor traffic entering and traversing the local network without introducing latency or bottlenecks. It works with security applications to instantly respond to alerts and block the movement of threats within a wired or wireless network. Unlike other solutions that operate down to the endpoint level, AMF-Sec can isolate compromised endpoints devices without the need to install agent software.

AMF-Sec uses best-of-breed intrusion detection applications to identify threats. When a threat is detected, the intelligent Isolation Adapter engine built into the AMF-Sec controller responds immediately to locate and quarantine the suspect device. Responses are configurable – for example, block the device, quarantine it on a VLAN, etc. – and comprehensive logging provides a clear audit trail on what has taken place. Remediation then can be applied by the network administrator so the device can re-join the network with minimal disruption.

Installation of AMF-Sec is easy because it interoperates with a wide range of physical and virtual firewall products, and no re-configuration is required. Two options are available for communication with network switches too: either with OpenFlow or AMF. AMF-Sec can use either method to control device access, which simplifies deployment and reduces the need for equipment changes.

AMF-Sec delivers real value by reducing network operating costs while constantly monitoring for threats and protecting the network.

In Conclusion

The conventional security approach concentrates on defending the network border, working on the assumption that it is the only way threats can enter the network. As we have shown, this is not true and companies that adopt this approach can be blindsided if they do suffer an insider attack. Whether the attack is malicious or the result of human error, the results can be devastating. Therefore, organizations must be well-prepared for insider threats in whatever form they take.

Allied Telesis automated solutions reduce mistakes and defeat malicious actions. Configuration automation helps to reduce errors by simplifying manual changes and security automation detects and responds to threats faster and more accurately than any human can.

-
- ¹ <https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/>
 - ² <https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/>
 - ³ https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf
 - ⁴ https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf (accessed Sep 2019)
 - ⁵ <https://www.dimensiondata.com/-/media/dd/corporate/content-images/pdfs/uncategorised/accelerate-your-ambition/network-barometer-report-2016.pdf> (accessed Sep 2019)
 - ⁶ <https://www.fiercetelecom.com/telecom/google-pinpoints-root-cause-sunday-s-outage>
 - ⁷ <https://pages.mediapro.com/2017-State-of-Privacy-Security-Awareness.html>
 - ⁸ Ponemon Institute Cost of Insider Threats Report, 2018

About Allied Telesis

Allied Telesis is a global leader in connectivity solutions with a vision to deliver zero-TCO (Total Cost of Ownership) solutions with smart tools that make networking easy for enterprise, government, education, and critical infrastructure organizations.

Our broad portfolio of product and services is ideally suited to build easy-to-use networking solutions that lower costs and reduce business risk. With innovative technologies and comprehensive features, we enable seamless delivery of voice, video, and data to empower innovation, increase business agility and help our customers gain a competitive advantage.

To learn more about the Allied Telesis solutions described above, as well as others we offer, please visit www.alliedtelesis.com or contact one of our sales representatives.