WHITE PAPER

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 three 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]
- **Human responses to threats** – IBM Security reported in 2019 that 77% of organizations do not have a cybersecurity response plan applied consistently across the enterprise.[5]

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.[6] 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.[7]

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.[8]

> *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.[9] 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.

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

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 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.

Human Responses to Threats

> *54% of organizations with cyber response plans do not test them regularly.*

Without doubt, stress and lack of training are the leading causes of human error. When both are combined, the potential for mistakes skyrockets and the organization is at its most vulnerable. Often this happens when the company is under cyberattack and time is of the essence, and without proper training, network admins make mistakes as they try to defeat the attacker. This happens more often than you might think. According to IBM Security, 54% of organizations with cyber response plans do not test them regularly.[10]

There are some industries that have developed effective ways to avoid the majority of human errors under stress. For example, airline pilots undergo rigorous and repeated training to simulate stressful situations, so that if they occur during real flights, pilots can calmly follow procedures and make the right decisions. We can follow their example and train our organizations to be prepared to handle a cyberattack calmly and without errors.

Various preparedness training methods exist but live simulations are the most effective, as the airlines have already proven. Table-top exercises are good for developing procedures and sharing knowledge, but nothing can replicate the stress of a live event like a realistic and real-time simulation.

The whole organization must know how to react correctly since many cyberattacks don't only impact the network. Ransomware demands, data theft, and business disruption threats will often contact other areas of the organization first. Acting correctly from the outset can shorten the attack duration and limit the damage, both financial and reputational. Therefore, the simulations we offer are not only for network administrators but also include representatives from legal, HR, finance, logistics, public relations, etc.

Our simulations run on the DECIDE platform that was developed by Norwich University Applied Research Institute (NUARI) as a tool to prepare financial institutions for cyberattacks. Using their experience, we have created a suite of training exercises that enable enterprises to test their attack preparedness and improve their processes and training as a result. Our real-time simulation exercises include personal identifiable information (PII) breaches, DDoS attacks, device backdoors, and more.

> *Acting correctly from the outset can shorten the attack duration and limit the damage, both financial and reputational.*

A Deeper Dive – The Allied Telesis Solutions to Overcome the Human-Caused 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, to automatically defend against threats that skirt the enterprise firewall, and to teach people how to respond to cyber threats quickly and appropriately. Let's take a deeper dive on each of these solutions.

The Autonomous Management Framework (AMF)

Allied Telesis' Autonomous Management Framework (AMF) 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 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 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 auto-backup reduces effort and the risk of errors by automatically managing the configurations for all devices in the network. Every day, AMF 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 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 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 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 automatically selects the correct configuration. If a new device hasn't been pre-provisioned, then AMF isolates the device until it has been successfully configured, either automatically by AMF or manually by the admin.

These various capabilities of the Autonomous Management Framework 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 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.

Employee Training Using the DECIDE Platform

The DECIDE Platform is the mechanism for delivering highly customized cyber awareness training consisting of live simulated exercises that enable workers to learn, or reinforce what they know, about task-specific risks. Allied Telesis and the Norwich University Applied Research Institute (NUARI) collaborated to develop the DECIDE platform around NIST security standards. The training exercises are delivered in classroom settings via a cloud service, so there is no hardware or software for customers to buy or install.

Envigilant Systems, the managed services arm of Allied Telesis, works with customers to construct the customized awareness exercises. The simulations are crafted to challenge people in scenarios that mirror their own daily tasks. For example, an employee in Finance might be presented with a directive to transfer funds and they need to decide if the order is legitimate or if it originated from a bad actor. An engineer might receive an email request from a colleague to share product design specifications and they must decide if this is a spoofed request attempting to steal intellectual property. The tests are customized to specific job roles to simulate the real work environment and to teach people to apply security best practices to their critical job functions. Employees learn about attackers' tactics, techniques and procedures (TTPs) that are indicative of a potential cyber-attack, as well as the appropriate ways their company wants them to respond to cyber incidents.

> *Everyone must be taught to be aware of cyber-risks and how to react appropriately when faced with a suspicious scenario.*

Following the training sessions, the results are summarized and a report generated of the organization's state of readiness to respond to cyber threats. This helps the organization fine-tune its policies, procedures and incident response playbook.

The simulated exercises are appropriate for any level of employee – including executives – who spend any amount of time online for their job roles. This is important because phishing and ransomware attacks are known to target non-IT people who might not recognize the TTPs of an attack. Everyone must be taught to be aware of cyber-risks and how to react appropriately when faced with a suspicious scenario.

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 blind-sided 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.

The most effective countermeasures to prevent human errors are frequent security awareness training and implementing best practices such as least-privilege, need-to-know, network segmentation, etc. However, it's wise to adopt a belt-and-braces approach that reinforces best practices with automated solutions to 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.

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.

[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
[5] https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them
[6] https://www.dimensiondata.com/-/media/dd/corporate/content-images/pdfs/uncategorised/accelerate-your-ambition/network-barometer-report-2016.pdf
[7] https://www.fiercetelecom.com/telecom/google-pinpoints-root-cause-sunday-s-outage
[8] https://pages.mediapro.com/2017-State-of-Privacy-Security-Awareness.html
[9] Ponemon Institute Cost of Insider Threats Report, 2018
[10] https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com

C613-08044-00 RevA