APPLICATION NOTE

Quick Tips on Security Resilience

While everyone knows that a security breach is a bad thing, many people do not understand that there are two ways to strengthen your network security. The first choice is to create multiple defenses against different types of threats. Unfortunately, you cannot defend against every threat. A second approach, security resilience, is a complementary approach to defensive security which addresses a security threat once it is inside the network.

Resilience, according to the Merriam-Webster dictionary, means “the ability of something to return to its original shape after it has been pulled, stretched, pressed, bent, etc.” From a network security perspective, resilience refers to the ability of an IT network to recover to normal, steady state operations after a security attack and breach have occurred. The resilience concept encompasses three components: information security, business continuity, and network/ organizational resilience.

Security resilience focuses on “after breach” activities. The reason for focusing on this strategy is simple — you want to reduce costs. These activities, if done right, will help you reduce the costs of a breach either directly by limiting the data stolen, or by decreasing the financial amount of each fine incurred, and in turn, minimizing bad publicity.

Overview

This brief provides techniques on how to improve the resilience of a security architecture.

Additional resources:

- Best Practices for Network Security Resilience
- Security Resilience The Paradigm Shift is Here
- Best Practices for Security Resilience
- How to Improve Network Security Podcast

KEYSIGHT TECHNOLOGIES

By implementing specific techniques, the following issues can be reduced:

- Threat discovery time
- Company risk
- Component recovery and validation time

Network visibility is the key to the solution. You cannot secure what you cannot see. A network visibility architecture empowers the security engineer with information to isolate security threats quickly; making visibility a central component of network security. Visibility is what allows you to optimize your network data capture and analysis techniques. A visibility architecture typically yields immediate benefits: elimination of blind spots, improved data flow to security tools, and maximum network and tool availability.

There are three layers to a visibility architecture:

1. The first layer is data access. This is where you will want to insert taps and bypass switches into the network, between the network data flow and your monitoring tools (or network packet broker), to improve the quality of monitoring data and time to data acquisition.
2. The second layer is the monitoring data manipulation layer. This is where you will want to deploy network packet brokers (NPBs) between those bypass switches or taps and the security and monitoring tools. The packet broker allows you to optimize the data sent to the tools. Once installed, you can perform various functions (as applicable) including out-of-band data filtering, Transport layer security (TLS) decryption, data deduplication, packet slicing, header stripping, and many other functions to optimize the data before sending to your monitoring and security appliances.
3. The third layer of a visibility architecture consists of the monitoring and security appliances. Examples include intrusion prevention systems (IPS), intrusion detection systems (IDS), web application firewalls (WAF), security information event and management (SIEM), and data loss prevention (DLP).

Application intelligence lets you look at the application level data — which applications are running on different portions of your network, how much data is flowing between different network segments, and geolocation of users.

This helps you in one of two ways — you can either directly see indicators of compromise (IOC), or the application data is sent to your IOC tool.

How to Reduce Threat Discovery Time

One of the first things you want to do after a security attack is to find out if your network was compromised. One common approach is to buy a security tool (SIEM, DLP, or IDS) that focuses on recognizing patterns and any unusual activity to uncover indicators of compromise. The tool needs network data fed to it by the packet broker. Besides a basic data feed, application intelligence lets you look at the application level data — which applications are running on different portions of your network, how much data is flowing between different network segments, and geolocation of users. This helps you in one of two ways — you can directly see indicators of compromise (IOC), or you can forward the application data to your IOC tool.

Automation is another important activity. A well-built NPB should also have the ability to respond to commands from approved external devices through a Representational State Transfer (REST) interface. REST allows you to automate responses to increase response times. The automated capability delivers a phenomenal time to respond to decrease the time to resolution.

Another way to improve resilience is with cyber range training. While cyber range training is general training, rather than specific to resolving a single breach, it provides IT and security personnel with tips and tools for performing forensic activities. It gives you the experience to recognize different categories of attacks. During or after a breach, you can respond more quickly with the knowledge of what to look for and where to discover IOC.

Threat hunting solutions are another critical component. Whether the attack is against your cloud or on-premises network, you need quick insight into all parts of that cyberattack. This includes analyzing data from all vectors. Third-party packet inspection analysis technology solutions then process the data.

Whether the attack is against your cloud or on-premises network, you need quick insight into all parts of that cyberattack.

This includes analyzing data from all vectors.

How to Reduce Company Risk

Another activity is to use a threat intelligence gateway. The solution takes the live threat intelligence capability to the next level and allows you to block suspect traffic proactively. Threat intelligence gateways are typically a defensive approach to prevent infiltration — all incoming traffic from known bad IP addresses is deleted at the edge of the network. However, if the IP address is not recognized as bad initially, malware can infiltrate the network. If an IPS does not capture the threat, then it continues into the network and does its dirty work.

However, the threat intelligence gateway should have a constant update process with new access lists. This means that should malware get into the network, the threat intelligence gateway still has the possibility of catching outgoing traffic to newly discovered bad IP addresses.

Network packet brokers deployed in an out-of-band use case have a couple of features that can also help with security resilience. One feature is SSL decryption, which allows the NPB to decrypt the traffic and send it to an out-of-band monitoring tool, like a DLP, IDS, or SIEM to find threats faster. Even though decrypted traffic may have been inspected initially as part of a defensive architecture and no issues were found, the traffic could still contain malware because the malware was missed by the inspection and it was not flagged, or it was flagged, and you did not have time to inspect the flagged traffic.

At this point, the traffic may need additional deep packet inspection by an IDS or DLP. Even if it has already done its damage, you still need to understand how it works, where it came from, and how it operates.

How to Reduce Company Recovery and Validation Time

The final benefit of security resilience is the ability to reduce component recovery and validation time. For instance, threat simulation tools allow you to see how a suspected threat behaves. Essentially, did you find everything or are there still traces of the malware left in the network and equipment?

Specific security threat simulation tools also use rich NetFlow information from an NPB to create a capture of relevant NetFlow-based information made during an attack. This allows you to get more specific data on the attack and how it took place. You can then replay that data in a lab to analyze the specifics of the threat.

Once you have an idea of what you are looking for, you can run a simulation in a lab to see how the threat behaves. Specifically, let's say you think you are the victim of a Heartbleed attack. You can use the simulator to accurately depict how that piece of malware will behave and then look for tell-tale signs on your network. The simulator shows you the specific registers compromised within your network.

A security threat simulation tool can also validate potential security fixes against a threat simulation tool to see if it works in the lab first, which delivers the confidence you need to perform the network rollout of the security breach fix.

A security threat simulation tool enables you to validate potential security fixes against a threat simulation tool to see if it works in the lab first.

It gives you the confidence you need to perform the network rollout of the security breach fix.

Network Security Solutions from Keysight

Network security resilience solutions allow you to deliver a faster time to resolution for security breaches. Specifically, you can recognize breaches faster, isolate security threats better, and repair the network as quickly as possible.

Keysight's network security solution involves using network packet brokers in conjunction with SSL decryption, application filtering, bypass switches, security threat testers, and threat intelligence.

Learn more about Keysight's network packet brokers, NetStack, SecureStack, AppStack, BreakingPoint, ThreatARMOR, bypass switches, and, tap technology along with the solutions that our technical partners offer.

If you want more details of the various use cases described, you can view a webinar on network security resilience, read an overview of security resilience, or access the definitive guide to network visibility use cases to learn more.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES