Fortify Your Cyber Threat Capabilities

The Government CISO Challenge — Getting to the Root of the Problem

The threat to national networks is higher than ever. Hidden threats can be lurking in the background of the network and you won't even know it. Missing just one piece of critical data can mean that your intrusion prevention system (IPS) misses a security threat and allows that threat to enter the network.

Sources of risk and confusion are everywhere for government CISOs. For instance, is the list below just a group of random security-related factoids? If not, how does a CISO correlate these items?

- You could be missing 60% of your security threats and not even know it.
- 70% or more of malware may now be hidden within encrypted data.[1]
- In the United States, Presidential Executive Order 13800 is driving government agencies to modernize and fortify their IT systems.
- 45% of respondents admitted to turning off features in security devices in order to improve performance, according to ZK Research.[2]
- The creation of new malware, ransomware and advanced persistent threats has not diminished in the last five years.
- 85% of mean time to repair (MTTR) is the time taken to identify that there is in fact, an issue.[3]
- According to the 2019 Verizon Data Breach Investigation Report, a breakdown of reported security attacks showed that 34% were due to insiders, 23% were nation state sponsored, and 39% were created by organized criminal groups.[4]
- According to Statista, in 2018 there were 31,107 cyber security incidents against federal United States agencies.[5]

Your SecOps team needs the right information and the right defenses at the right time. This reduces risk, wasted time and effort, costs, and creates the best opportunity to block a cyber-attack.

Seven Network Fortification Tactics for Government CISOs

Does this mean that your SecOps team needs more help to fortify the network? Probably — most teams do need some help.

Here are seven different tactics to consider that can strengthen your government agency network:

1. Validate that your security and monitoring equipment function correctly. For instance, some network packet brokers (NPBs) drop packets which means that your IPS tools can miss 60% or more of the security threats.
2. Maximize service continuity and network uptime of security defenses with external bypass switches. Built-in bypasses are worthless if you need to completely replace the security tool(s).
3. Implement a multi-layer defensive architecture. This includes the use of inline security solutions with NPBs, SSL/TLS decryption, and self-healing architectures.
4. Deliver functionality that supports and enables cyber resilience by looking for faster attack diagnosis, faster testing of potential fixes, and faster network recovery.
5. Strengthen defensive security measures using application intelligence and NetFlow information to enhance threat identification activities.
6. Reduce your compliance risks by using an NPB with application intelligence to mask sensitive data and detect unauthorized offsite data storage.
7. Protect network security from eavesdropping by other individuals and foreign governments with air gapping technology.

To implement use cases relevant to government agencies, Keysight offers a wide range of security solutions. Reach out to us and we will show you how to fortify your network against multiple threat vectors.

References

1. Omar Yaacoubi. "Keeping Up With Encryption in 2020," Security Boulevard. April 6, 2020.
2. "The Importance of Lossless Network Visibility," Ixia, A Keysight Business. Nov. 8, 2016.
3. "Making the Shift to Strategic IT," Ixia, A Keysight Business. July 25, 2018.
4. "2019 Verizon Data Breach Investigation Report," Verizon Enterprise Solutions. May 8, 2019.
5. J. Clement. Jan 17, 2020. Statista Inc. https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/

Learn more at: https://ixia.keysight.com/solutions/segments/government-solutions

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

https://ixia.keysight.com/contact/info