Are You Protected Against **Insider Threats**?

When it comes to network security, the attitude is: Assume breach. Hacking methods are continually evolving, and often hackers are multiple steps ahead of the security teams building defenses to keep them out. However, many of the network's greatest vulnerabilities are already inside the firewall. Whether it's someone with malicious intent or dangerous ignorance, the network needs to be protected from these insider threats. The best way to do that? Know what needs to be monitored in your network and what tools can get the job done.

2,500 — According to IS Decisions, the number of **internal security breaches** occurring in the U.S. business every day.

43% — The percentage of data loss **internal actors** were responsible for according to security professionals surveyed in Intel Security's Grand Theft Data Report.

47% — The percentage of **IT decision makers** concerned with internal security breaches by employees, according to Cisco's 2016 Annual Report.

Who is Responsible for **Insider Threats**?

Bad Actors

These are the employees who know what they are doing when stealing data from the company. Often the motive is easy money. According to the 2015 Verizon Data Breach Investigations Report, financial gain and convenience were the motivating factors in 40 percent of insider incidents.

Negligent Employees

These employees unknowingly put the company at risk of a breach through their actions or looseness with information. Often, these are the employees who download malware, fall victim to phishing scams or over share on social media. Each of these are things an experienced cybercriminal can exploit when attempting to gain access to a network.

Combat Insider Threats with **Best Practices & Monitoring**

Other than creating policies that outline guidelines for password creation, use of public Wi-Fi, and what should or shouldn't be shared on social media, protecting your network from insiders comes down to limiting access to the network and monitoring traffic that is already inside.

To ensure data is safe, the organization needs to build security in layers and use multiple tools and other hardware to monitor the critical data flowing through its network. That includes data coming in as well as data going out, often one of the first signs that the network may have been compromised. Layered security might include:

An Intrusion Protection Systems (IPS), more commonly known as a firewall, to keep out known threats.

An integrated Intrusion Detection System (IDS), which is actively looking for incidents or security policy violations by monitoring the network on a 24/7 basis. Think of it as a home-alarm system for an IT network.

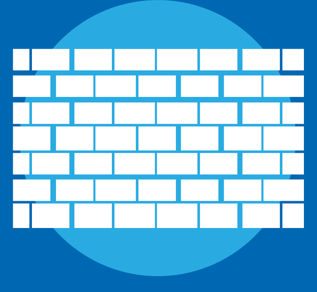
A Data Loss Prevention System (DLP) that raises alerts to sensitive information leaving the network.

Several tools that scour traffic looking for the telltale signs of hacking or the signatures or domains of known security threats.

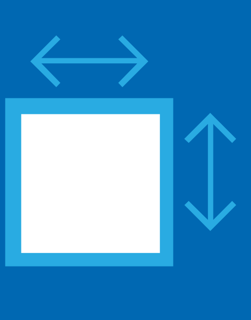
The biggest concern of a security team trying to combat insider threats might be one of physics: How to give so many security tools access to the same network traffic in real time?

Monitoring Starts **with Architecture**

When implementing an optimal solution, start with a holistic, top-down plan of traffic needed for specific monitoring tools. Understanding data needed for security analysis vs. application performance vs. network troubleshooting will lead to better planning for placement of SPANs and/or TAPs. TAPs offer visibility to all data without taxing system resources of networking gear. A network monitoring switch can combine all necessary monitoring points and tools in a centralized or distributed architecture depending on requirements. The right network monitoring switch offers three things:



Scalability



Scalability helps meet the needs of network size and tools deployment, involving appropriate port count. With APCON's IntellaFlex XR architecture, you gain flexibility to deploy appropriate capacity and functions as your network grows. That means scaling from a 1RU to a 14RU chassis and providing anywhere from a few ports to 504 non-blocking ports. The architecture offers flexibility of software configurable 1G/10G ports along with 40G and 100G port options. Compatible firmware, blade reuse and power/controller redundancy ensures robust operation and investment protection across different sized networks.

Advanced Features

Advanced features provide utility and efficiency in monitoring tool investments. Multistage filtering and port tagging ensures the appropriate data reaches the correct tool. Packet slicing, packet deduplication and protocol stripping enables the tool to receive only the packet information of interest to optimize analysis performance. This keeps the tools from becoming oversubscribed, reduces the unnecessary replication of sensitive data, helps companies meet regulatory and compliance requirements, and maximizes the company's capital investment.

Management Tools

With complex network environments and port counts reaching the hundreds, management becomes a crucial element of practical deployment strategies. APCON's WebXR is a web-based graphical interface that can manage connections, receive appropriate alerts and plan upgrades. APCON's TitanXR provides a single, centralized point of management for network monitoring in multi-switch and virtual environments.

Monitoring for the **Network**

Today a security breach can result in costly downtime, requiring businesses of all sizes to make sure they are protected from threats of all kinds. With APCON's data aggregation and filtering solutions, companies will increase their network visibility and enhance their network security and performance.

Want to learn more about protecting your network from insider threats?

DOWNLOAD THE EBOOK

SOURCES

1. http://net-security.org/secworld.php?id=16379
2. https://www.riskbasedsecurity.com/reports/2014-YEDataBreachQuickView.pdf
3. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?sub type=WH&infotype=SA&htmlfid=SEW03055USEN&attachment=SEW03055USEN.PDF
4. http://www.isdecisions.com/insider-threat/statistics.htm
5. http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_59084.pdf
6. https://www.cloudbric.com/blog/2015/11/are-you-protecting-against-internal-data-breaches/
7. http://www.mcafee.com/us/resources/reports/rp-data-exfiltration.pdf
8. http://www.cisco.com/c/dam/assets/offers/pdfs/cisco-asr-2016.pdf

APCON Solutions for Networks

www.apcon.com