Jacob Thankachen 6/11/2015

Know Who's on Your Network and What They are Doing

Maintaining network security has never been more challenging than it is right now. Traditional network perimeters are beginning to blur in the face of consumerization, the rise of mobility, migration to the cloud, and the Internet of Things.

The pursuit of business agility has driven these trends, and they offer tangible benefits, but in the rush to adopt them, information security has been left behind.

According to the Pricewaterhouse Coopers, Global State of Information Security Survey: 2015, the number of detected incidents reached 42.8 million last year. That's an increase of 48% over 2013, and the total financial losses attributed to those security breaches were up 34% on the year before.

Ever more stringent regulatory guidelines and compliance standards are also putting businesses at risk of legal liability in the event of a successful cyber attack.

Last year the Ponemon Institute suggested the average cost of a data breach was $3.5 million. It's vital that companies take preventive measures, and that means investing in network security.

Time to Modernize

Too many companies are still reliant on a muddled mixture of legacy security tools and processes that are simply not equipped to cope with the demands of cloud computing, BYOD, virtualization, and remote working.

The days of static ingress and egress points are gone. To achieve real enterprise-class network security, you need granular controls, a flexible tool set, and real-time oversight.

There's a tendency to concentrate on external criminal attacks, but many network breaches can be attributed to malicious insiders, or plain, old human error.

As the potential attack surface expands, it's time to formulate a comprehensive strategy, and adopt a security solution that covers all the bases.

Visibility and Control

Any solution that you do adopt, must be capable of integrating with existing systems. You don't want to create a huge policy burden, and start filtering and banning devices and apps.

The first step is to achieve full visibility over your network traffic. Control access to network resources based on authenticated user identities.

Secure tunneling through VPN with encryption allows safe access to the corporate network from any device, enabling remote workers or partners to work wherever and whenever they need to.

To prevent data leakage you'll want control over application security. Automated scanning should flag and block any anomalous traffic, shutting off potential inroads for malware.

To ensure that no data leaks out, Instant Messaging and email applications must be monitored, and a wary eye cast on file transfers.

You should strive for central control, but remember the importance of security management that your CISO and IT support can grasp. Software that's too complex can lead to serious configuration errors and end up causing problems.

Every organization is different, so customization is key.

Collecting Data

You might be able to see who is on your network and what they're up to at any given time, but compliance requirements often dictate that traffic is logged and reported. A centralized system that produces a clear audit trail across locations is desirable.

Consider that many breaches and successful cyber attacks are not discovered for days, weeks, and sometimes even months after penetration. Collecting, aggregating, and analyzing data can help you to uncover suspicious activity, and it gives you a trail to investigate in the event that there is an incident.

It's also worth remembering, that network monitoring isn't just about security, it can also help you reduce latency and maintain stability as you scale. The right metrics will offer important insights into how to leverage your hardware for best performance.

Continuous Network Monitoring

It doesn't matter what size your business is, or what industry you are in, if you can't answer the question — Who is on your network and what are they doing? — then you're asking for trouble.

The fact that you can't plug every gap, and shut down every vulnerability in the various software tools you employ, makes your network monitoring capability even more important.

By understanding the flow of data in and out of your organization, you give yourself the best chance of catching any potential breaches in real-time. Being compliant with security standards, dramatically reduces the risk of legal liability, and the potential cost of an incident.

You'll also be safeguarding the company from internal dangers, not just external threats. In short, it's time to reconsider your network monitoring.

About the Author:

Jacob Thankachen is AVP Sales & Operations North America for Cyberoam, a Sophos Company and global security appliances provider offering physical and virtual networks Next-Generation Firewalls (NGFWs) and Unified Threat Management (UTM) appliances.