NETWORK SECURITY FOR BIG DATA NETWORKS

Whitepaper | March 2015

ENTERPRISE NETWORK SECURITY IN THE AGE OF DIGITAL ANARCHY

The year gone by witnessed a spate of malware attacks and network breach incidents that ambushed world's best guarded enterprise networks at global corporate giants and several military, government and critical infrastructure establishments. Malware mayhem continues and cyber-crime and attack methods continue to evolve. In an exceedingly digitally connected world, one small mistake or a click event can trigger an influx of sophisticated attacks in enterprise networks, leaving businesses wide open to evolving threats and cyber security risks.

Researchers, analysts, bloggers, journalists all have offered varying theories and analysis into this growing menace of evolved attacks, citing presence of critical security gaps in IT and network environments as the most significant vulnerability, putting organizational networks at greater risk.

Outline

The whitepaper discusses how the onslaught of disruptive technologies such as cloud, BYOD, virtualization and increasingly collaborative and open networks have left businesses in lurch, making them devoid of adequate security controls and visibility into user actions and network events.

Shedding light on how IT is impacting businesses while creating unprecedented challenges in securing the "Deperimeterized Enterprise", the documents highlights the growing importance of actionable security intelligence.

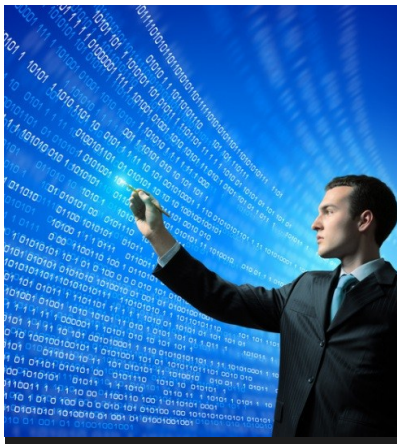
"Businesses and organizations emerge increasingly connected and digital, and at the same time, security environment continues to grow more complex"

Security blues in a De-Perimeterized World

Network security is becoming nearly unmanageable for most CSOs, CISOs and other security managers. For security executives, it has turned out a catch-22 situation, for on one hand, threats and attack methods are increasing in frequency, scope and severity and on the other hand, monitoring connected networks and user activities in a drastically evolved technology landscape is turning more stressful and ironically a thankless job at the same time.

IT and Security decisions turning into a boardroom battle

Internet brings us a digital economy and other avenues like cloud, virtualization, mobility, BYOD, IoT ecosystem and more. Progressive enterprises and established organizations alike yearn to seize this opportunity and catalyze unprecedented operational efficiencies and technology capabilities for their workforce, partners and customers. But there's a flip side too. Most CXOs remain at loggerheads in turning the disruptive into productive. This is because there's a lack of understanding into how security ties with business and IT / technology decisions. For example, a CSO and a CIO may argue over a question -whether going for cloud or virtualization can lead to new security challenges!



Developing an eye for detail

Aligning CIO and CSO interests requires finding the right solution around below aspects,

- Understanding critical IT and Network security gaps
- Primary causes that lead to security weaknesses
- How new security risks and challenges emerge from technology decisions (cloud, virtualization, BYOD etc)
- Potential risks and outcomes of such gaps
- Measures to narrow down IT security gaps
- Baseline security needs of the organization
- Correcting security posture by harmonizing security, compliance and productivity needs

Enterprise security teams want to transition from reactive to predictive / preemptive security

Cyber criminals behind evolved attacks and malware campaigns are not naive, basement hackers. They are skilled threat actors and they feast on security gaps in enterprise networks and exploit 'users' as attack vectors. And most organizations struggle to fathom whether their users pose as threat actors or attack vectors! Indeed there's an improved state of awareness and CXOs realize that besides external threats, insider risks and user driven actions too can prove lethal for their mission-critical networks and may jeopardize sensitive and classified data assets. As a result, stand-alone security solutions like firewall, IPS and VPN are giving way to integrated security solutions with actionable security capabilities.

Many organizations have begun leveraging big data analytics tools to capture early signs of specific user actions or network event patterns that may hint at a possible ongoing attack or anomaly.

CXOs understand that most security paradigms fall short in combating insider threats and user-triggered risks. Winds of change in enterprise security clearly reveal growing importance of analytics and actionable security as a key priority besides cloud, virtualization and mobility to cope with security challenges concerning audit and compliance, data protection and unauthorized access.

User Threat Quotient

Today, every enterprise generates lots of data, with ample clues, but the information remains incomprehensible. Cyberoam with its User Threat Quotient reporting capability models user behaviour to harness big data information on network events and user actions to spot risky users and trends, resolving the challenge of finding a needle in haystack. At a time when insider threat is reaching criticality, such an approach can be seen as a new Darwinism in IT security.

User Threat Quotient (UTQ) harnesses information derived out of network traffic and offers patterns of user behavior to determine risky users in a network. UTQ is available on Cyberoam’s Next-Generation Firewall and UTM appliances.

THE USER THREAT QUOTIENT HELPS CSOs / IT SECURITY MANAGERS BY:

- Spotting risky users at a glance without manual efforts to co-relate network logs and reports
- Facilitating corrective actions by fine-tuning user policies and managing risks arising from privileged users
- Eliminating the risk of error and oversight while dealing with huge amount of data contained in network logs and reports
- Eliminating the need for SMBs to invest in separate SIEM tools to spot risky users
- Enabling investigation into the spread of risk within the network with useful insights into network activities of risky users
- Removing complexity in analyzing terabytes of logs to identify user behavior by making actionable security intelligence readily available
- Allowing administrators to identify and educate users who pose security risks

Healing the Achilles' heel in Big Data networks

Businesses that suffer data breach incidents or network intrusions can act in haste and put the blame on firewall providers while citing some help from regulatory norms. However, the irony is that both data security laws as well as IT and network security practices at many organizations have not been able to keep up with the pace of evolving technology and attack methods. Surviving continued blitzkrieg of disruptive technologies requires adequate awareness of security. But we can draw from eye opening evidence that reality is different from what's needed. The Target breach and recent massive hacks into Sony and the U.S. Central Command (CENTCOM), and just about every other major attack are corroborating that poor security awareness is costing organizations a lot of money and reputation. Many security surveys and findings from breach investigations reveal that businesses lack understanding on baseline security needs and do not have adequate visibility or tab on user activities and network events. Today's organizations are big data companies and there's a need to revisit security posture and fill security gaps. Notwithstanding the fact that most security providers remain diligent in enabling timely patches, advisory, threat intelligence and other crucial inputs, it is for organizations to ensure that there's no Achilles' heel in their network or IT infrastructure. This remains key in thriving with confidence while embracing a bold new change amidst digital anarchy.

Cyberoam®
A SOPHOS Company