Infoblox
CONTROL YOUR NETWORK

WHITEPAPER

Protecting your enterprise network:

Security challenges, costs & solutions for IT practitioners

Introduction

More than 90% of enterprises have reported network security breaches — and the average data breach for a U.S. company now costs an average of $5.4 million per incident.

In the last few years, protecting business assets has become much more difficult to protect as the "bad" guys continue to evolve their attacks to evade IT defenses. When you add into the mix employee-owned mobile devices and cloud-based services, which require networks to be more dynamic than years past, traditional network security tools and practices are simply no longer enough to ensure protection. Nowadays, businesses are also coping with more destructive threats designed to steal competitive information and damage companies in search of profit — or even political advantage.

The threats are real, the costs are high, and no company is immune.

As early as 2011, enterprise network breaches were reported in more than 90% of surveyed companies, according to the Ponemon Institute. Ponemon's *2013 Cost of Data Breach Study* reveals average losses of $5.4 million per incident in the U.S. More than two-thirds of those costs (68%) are indirect. Anju Soni, a principal at Booz Allen Hamilton, warned that network intrusions often lead to reduced profits, reputational damage and shareholder mistrust — not to mention "downstream operational and legal expenses, often coupled with loss of brand equity."

Clearly, today's evolving threat landscape requires enterprise IT not to "sit tight" in its security infrastructure. Even previously state-of-the-art layered security solutions (often called "defense in depth") may not be up to the task. These strategies protect network endpoints with anti-malware software and secure the network itself with traditional IP-level firewalls. But the latest threats exploit gaps in that coverage. As a result, enterprise IT needs additional layers of security for the network itself — including more powerful network management tools and more robust network infrastructure. Domain Name Servers (DNS), in particular, need to be secured with a hardened operating system and hardware to reduce hacking. And new methods — such as DNS firewalls — are required to block DNS queries for "bad" domains.

A new kind of threat

Over the last few years, three factors have combined to attract organized criminal elements to hacking:

1. There's real money to be made — in several different ways.
2. There's a very low risk of getting caught.
3. There are readily-available hacking tools that anyone can modify to suit their purposes.

Today, profit-oriented criminals use infected computers to create bot-nets — giant armies of remote-controlled servers and computers that they "rent" out to anyone who wants to launch Distributed Denial-of-Service (DDoS) attacks. Call it DDoS for hire!

Criminal groups also sell and customize hacking kits with source code for various kinds of malware that make it easy for almost anyone to launch attacks.

The explosion of mobile and wireless devices makes it increasingly difficult to know who is on your network — and what they are doing.

Beyond *criminal* hackers, foreign *governments* — from China to Iran to North Korea and elsewhere — have now been implicated in large-scale hacking attacks. Recent targets include Google, *The New York Times* and *The Wall Street Journal*, as well as various government networks. These kinds of Advanced Persistent Threat (APT) attacks go far beyond script kiddies releasing random malware. They come from well-financed organizations that identify and attack specific high-value targets over extended periods of time.

That means that even if you clean up the original infiltration, the threat continues — especially since the attackers have probably mapped the network and server infrastructure to identify other vulnerabilities. And while you may have changed a larger number of logins and passwords, just missing one is all it takes for the process to repeat itself. They may even have hidden back-door software on the network so that they can continue to control and manage that network infrastructure. As a matter of fact, one outside security vendor that was trying to clean up an infected environment found malware on printers and thermostats!

Despite their potential to wreak havoc, cyber attackers face very little risk of prosecution. Many victims prefer not to advertise network breaches. And because attacks often cross national borders and may involve state-sponsored entities, local law enforcement often finds it difficult to address these crimes.

Vulnerabilities

In addition to new threats, the dramatic increase in the number and types of devices connected to corporate networks is creating new vulnerabilities. (In 2012, for the first time, mobile devices outsold PCs and are making their way into the enterprise via the Bring Your Own Device "BYOD" trend.) Rampant use of enterprise-wide mobile and wireless devices makes it increasingly difficult to know what devices are on the network and what they are doing.

Traditional network endpoints, like PCs and laptops, typically have some form of anti-virus software installed. However, most smartphones and tablets have no anti-malware protection — no anti-virus, no firewall, nothing. Worse, the very nature of these devices encourages users to hop on whatever wireless networks may be available, whether they're secured or not, making it very easy for them to become infected — and to spread that virus throughout to the enterprise network.

Even as Windows devices continue to improve their security, mobile malware jumped 163% in 2012 — with Android the target of some 95% of the infections. According to the NQ Mobile *2012 Security Report*, there were more than 65,000 pieces of Android malware circulating in 2012, infecting more than 32 million Android devices. (Apple's iOS and Blackberry devices have experienced far fewer malware issues due to their smaller global market shares, but also because their manufacturers offer continual updates and more closely restrict what programs they can run.)

In addition to mobile malware, attackers increasingly use mobile devices to gain access to enterprise networks because wireless access makes it more difficult to tell legitimate connections from rogue users and attackers.

Stolen and lost devices present another attack vector. A purloined device could offer complete access to enterprise networks and applications — not to mention a cache of the owner's personal information. Even when secured with a password, it's often possible for experts to crack the access code — especially if they know something about the device's owner.

The DNS vulnerability

DNS is becoming a dangerous — and often overlooked — security gap not covered by conventional security technologies.

All of these challenges lead to the same result: unauthorized access to the network. In many cases, IT staffers have no idea which devices are being used on their network at any given time — never mind what domains are being accessed. Authorized users could be using unapproved — and vulnerable — devices, or unauthorized users could have commandeered authorized devices. And if you don't know who's on the network, there's a good chance you have no idea whether or not they belong there or if they're behaving properly.

The increasing reliance on Domain Name System (DNS) infrastructure can create enterprise-wide IT weaknesses. Many enterprises rely on just a few DNS servers to route traffic within their internal network, as well as to access the open Internet, but most never gave any thought to the network vulnerabilities DNS servers create. Generic, low-cost, Windows-powered DNS servers get stuffed in racks in the data center with no special precautions. The idea was: "It's low cost, it works, it's fine, don't bother me, focus elsewhere."

Yet attacks that disrupt this small group of servers can easily serve the purposes of those who utilize or attack it. DNS is becoming a dangerous — and often overlooked — security gap not covered by conventional security technologies.

In the last few years, criminals have increasingly exploited DNS as a window into enterprise networks. It's like spinning a wheel over and over again until the malware locates a "bad" domain. The malware makes a request for a certain domain, and if that doesn't give it access, it just "spins the wheel" and tries again — over and over and over again until it finds a way in. Once it has access, the malware can download additional software to expand or change the attack or extract information.

DNS servers are also targets for Distributed Denial of Service (DDoS) attacks. Attackers program a botnet to make certain DNS requests to a certain server, spoofing the source of the request so the DNS server responds back to the targeted servers. The idea is that the sheer volume of the requests overwhelms the relatively few DNS servers that the company relies on to let internal users find their way out to the Internet.

A successful DDoS attack overwhelms DNS servers and impairs legitimate Internet traffic from getting out of the business — a problem that can cripple most modern organizations. These days Internet access isn't just surfing the Web and sending emails — it's also voice calls that use Voice-over IP (VoIP) and access mission-critical Software-as-a-Service, or SaaS, applications (including Salesforce, SAP, Oracle, NetSuite and even productivity apps like Microsoft Office 365 and Google Apps). Many cloud-based storage services (like DropBox and Box) also rely on Web access. DDoS attacks can also impact the company's e-commerce and other online operations — leaving many businesses extremely vulnerable to attacks that can render them inoperable.

Challenges: Network management and visibility

Modern multi-vendor networks make it difficult to track overall network usage and vulnerabilities.

The combination of increased network complexity and new vulnerabilities makes it more important than ever for enterprise IT practitioners to recognize threats in real time, build a comprehensive picture of the threat, and alert the right IT resources to respond promptly and effectively.

Unfortunately, modern multi-vendor networks make it difficult to track overall network usage and vulnerabilities. While each vendor's tools may offer glimpses of what's going on, there's often no way to get a full picture — making it very difficult to see what's open, what's blocked and what's the best path between various points in the network.

If you've got a Cisco firewall but Juniper routers, for example, the Cisco network management tools cannot see the Juniper routers' access policies, and vice versa. And if the vendor management tools can't even see each other, they definitely can't monitor policies and rules, let alone correlate or manage them with each other. This inability to cross-correlate access policies between multiple network management tools creates critical blind spots.

Manually managing a multi-vendor network with single-vendor tools means network admins don't have a complete picture of all the devices on the network, their relationships and policies of what they can and cannot access (white lists and black lists).

Admins may find themselves manually creating time-consuming, hard-to-maintain and easily outdated spreadsheets or Visio drawings to track what is allowed or blocked on their networks. But that's only an approximation — someone's best guess as to what is connected to what at any given moment — extrapolated from individual policies to the network as a whole. What's more, there's no way to ensure that the manual list stays current with network changes and updates. In other words, network administrators end up managing network access based on guesses, not real knowledge.

Making things worse, in many cases there's no way to test or model proposed network changes before deploying them to production. If those changes cause problems, network admins may find out only when the user complaints start rolling in. That's bad for users, obviously, but also adds to IT's management burden and tarnishes its reputation.

Solutions: More robust DNS and improved network management

To address these threats and challenges, enterprise IT practitioners need:

1. **Robust, scalable, and redundant DNS infrastructure** to resist security threats and provide greater resiliency against attacks;
2. **DNS firewalls** to close the gap left uncovered by traditional security solutions;
3. **Greater network visibility** into the devices and users connected to an enterprise network;
4. **Comprehensive, cross-vendor network management tools** that provide "single pane of glass" reporting and flagging of security policy across the entire network, no matter which vendors' equipment is affected;
5. **Security device management** technology that can spot unplanned events or provisioning errors before they affect a production network.

1. DNS infrastructure

To properly protect the core corporate network services, DNS, DHCP (the Dynamic Hardware Configuration Protocol) and IP address management should be integrated on a single platform, with both hardware and software designed together to minimize security vulnerabilities — to a level that can be demonstrated by Common Criteria Level 2 certification.

On the hardware side, that means over-provisioning DNS capacity, enabling DNS servers to handle DDoS floods, traffic-rate limiting, and load distribution, as well as making it easier to control access by limiting the number of ports that users can connect to.

On the software side, it means granularly provisioning network access and permissions. All users should not have super-admin privileges that give them root access to the network. Depending on their role in the organization, people, devices and applications should be given the ability to see and access only the parts of the network that they need.

In addition, to help prevent DNS spoofing, DNS servers should have cross-certification to each other, so they can confirm that the server they're connecting to is the right one for resolving DNS queries.

2. DNS firewalls

DNS firewalls are not a traditional part of network security infrastructure, but that needs to change. DNS firewalls give enterprise networks the ability to block DNS queries going to known bad domains — or to restrict DNS queries (driven by malware or legitimate users) to approved domains. In addition to blocking bad queries, the DNS firewall should be integrated with DHCP to capture and correlate the IP address and related metadata (including device type and when it accessed the network) of the devices. These technologies are designed to naturally capture this information and, in order to pinpoint and remediate compromised devices on the network, IT should be enabled to take advantage of it.

3. Network visibility

Managing IP addresses and network policies via spreadsheet or Visio drawings is not a scalable solution for modern enterprise networks. Integrated, automated network management applications built into the network infrastructure are essential to tracking changes and capturing valuable security information.

IT practitioners need to know what the change was, who made it, and when. If the change violates network policies or opens a security hole, they need to be alerted — via email and/or in the appliance's user interface — so admins can take prompt remedial action. And the rules governing those alerts need to be automatically updated to account for the latest updates to network policies.

4. Cross-vendor network management tools

The key to effective network management is being able to see everything in one place — no matter what vendors' products are involved. This so-called "single-pane view" is essential to making sure that devices don't fall through the cracks and security vulnerabilities can't hide in the blind spots between single-vendor management tools.

But it's not enough to be able to discover new devices — network administrators also need to be able to see all of the network access rules and policies to properly understand the relationships between the devices on the network.

This is not a one-time-only task — the network must be monitored 24/7. Any out-of-spec changes must be immediately identified so admins can find and address the issue before it causes potential holes — or breaks or changes network paths.

Management is more than monitoring and alerts, of course. IT practitioners also need to make changes across multiple devices from multiple vendors. That's a big deal because writing, configuring, and pushing out changes to a Juniper device, for example, is very different than just updating a single Cisco router or switch. Handling each vendor's equipment separately requires multiple experts and invites confusion.

Automating that process of implementing network policies, including white lists and black lists, saves IT time and cuts down on errors. Better still, when that process is integrated into network management, IT practitioners can be confident that access privileges to routers, switches and firewalls are properly configured.

5. Test environments

Finally, IT practitioners need the ability to model their proposed network changes, so that they can see what's going to happen before the changes are deployed to production. Ideally, changes should be tested and then scheduled to go live at a specified time, but only after receiving the proper approvals.

The idea is to let help desk personnel decide that, "Oh, this group of users needs access to this application? Here, I'll write a policy that specifies the path via this protocol, and then we'll set it to be ready for Monday morning. We'll apply it Saturday at 9 p.m."

So far, so good. But the next step is to make sure those changes are reviewed by management to make sure they don't violate network policy standards. If the changes are approved, they get applied Saturday night. If not, the changes are denied and an alert is generated to make sure the issue gets resolved.

Conclusion: New threats and challenges call for a new approach to network security

Modern network management can deliver greater network visibility — even in multi-vendor environments.

Enterprise IT security threats continue to become more targeted and more dangerous, security challenges are getting even more complex, and the costs of security failures keep going up. Business as usual can no longer protect enterprise networks against these threats — much less what's coming tomorrow.

Enterprise IT needs to act now to address the challenges of ubiquitous mobile device access, for-profit hacking, Advanced Persistent Threats, DNS server vulnerabilities and complex multi-vendor network management.

Fortunately, new tools are available to build more robust DNS infrastructures, including DNS firewalls to close security gaps. Modern network management can deliver greater network visibility — even in multi-vendor environments — including the ability to test and manage deployment of network changes.

Adopting these new tools and procedures is no longer optional — the risks and costs of network breaches are simply too great.

About Infoblox

Infoblox (NYSE:BLOX) helps customers control their networks. Infoblox solutions help businesses automate complex network control functions to reduce costs and increase security and uptime. Our technology enables automatic discovery, real-time configuration and change management and compliance for network infrastructure, as well as critical network control functions such as DNS, DHCP, and IP Address Management (IPAM) for applications and endpoint devices. Infoblox solutions help over 6,500 enterprises and service providers in 25 countries control their networks.

CORPORATE HEADQUARTERS:

+1.408.986.4000

+1.866.463.6256

(toll-free, U.S. and Canada)

info@infoblox.com

www.infoblox.com

EMEA HEADQUARTERS:

+32.3.259.04.30

info-emea@infoblox.com

APAC HEADQUARTERS:

+852.3793.3428

sales-apac@infoblox.com