FEB 2016

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the February 2016 edition of In the Boxing Ring

This month we talk about High-Value Targets, ie **Point of Sales**, **Credit Cards** and **Customer Information**. In today's threat landscape, malicious hackers and cyber criminals are targeting these assets in order to steal your information for financial gain. On pages 2-4 we discuss in detail how we can mitigate these threats and how you can prevent yourself from becoming a target.

On pages 5–6, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. Based on Sunset Policy, we will continue to support, Network Box 3 until at least late 2018.

Finally, Network Box has been named as a finalist in six categories in the upcoming Info Security Global Excellence Awards, and also named in two categories for the SC Magazine U.S. Awards. In addition, Network Box Germany officially became a partner with comTeam.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
February 2016

You can contact us here at HQ by eMail (nbhq@network-box.com), or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

- twitter http://twitter.com/networkbox
- facebook http://www.facebook.com/networkbox
  http://www.facebook.com/networkboxresponse
- Linkedin http://www.linkedin.com/company/network-box-corporation-limited
- Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

NETWORK BOX

High-Value TARGETS

Point of Sale, Credit Cards, Customer Information

Long gone are the days when a computer virus would pop up a message on your screen "Your PC is now Stoned!", or humorously display a trail of worms on your desktop. Today's malware authors are mercenary in their approach, and primarily motivated by both the expansion of computer networks under their control and theft of your information. In particularly, they are actively targeting point of sale units, credit card, user credentials, and other systems holding customer information.

In the words of Geena Davis (as Veronica Quaife) in the film "The Fly", it is time to *"Be afraid, be very afraid"* and to take practical steps to lock down and secure such high value targets in your network. In most situations, in particular if you are already protected by Network Box equipment, you already have everything you need to do the job – you just need to get the policies defined, implemented, and ongoing monitoring in place. This article should give you some ideas and a plan to approach the problem – something we call the four I's:

- *Identify*
- *Isolate*
- *Implement*
- *and Incident response*

Identify

Having recognized that this could be a problem affecting your organization, the first step is to identify the high risk target systems you have in your network. You do this by conducting a risk analysis of the information in your network, and the machines where that information enters, is stored, is processed, and leaves. Pay particular attention to customer private information, account information, credit card, point of sale, authentication, and banking systems (including those that store/use external bank authentication).

Such a risk analysis can be either conducted purely internally, or you can employ a third party consultant to assist. Both have their benefits and drawbacks – a third party consultant brings a fresh look at your systems, but doesn't have the in-depth knowledge that your own team has.

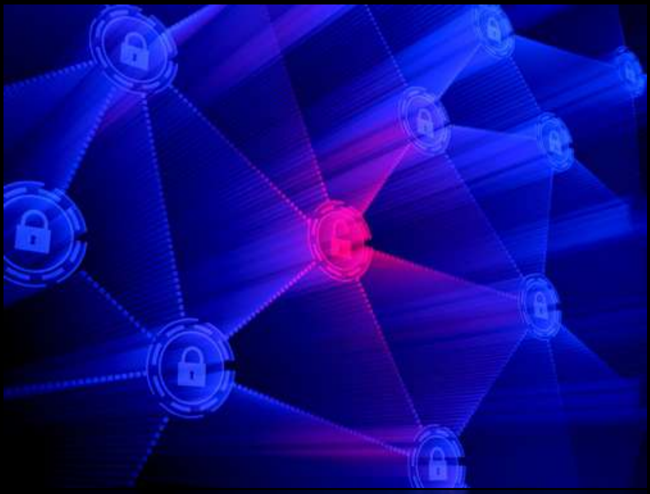
Whichever your approach, the purpose of the exercise is to identify the systems of greatest concern so that specific protection mechanisms can be brought to bear. Security will always be a trade-off against convenience, but for these key high-value systems, the scales should always tip towards the side of maximizing security (even at the expense of sacrificing convenience). Risk assessment helps you identify the high value (to an attacker) systems, so that you can concentrate your efforts.

Isolate

Isolation is the technique of physically isolating these high-risk systems. It is not sufficient to merely partition these off as an IP address range, or run multiple subnets on the same physical wire. You need to physically separate these high-risk systems from the rest of your network.

The purpose of such isolation is to ensure that a penetration of your lower-value (perhaps easier to penetrate) networks, cannot cross across to your high-risk systems. Equally importantly, proper isolation ensures that you can implement restrictive policies to control the information flow not just into, but also out of such isolated networks.

Inter-connection of such networks to the Internet and/or internal systems is normally acceptable as a day-to-day requirement – but such interconnections must be via equipment that can control policy in a highly granular manner, and should normally include Intrusion Detection and/or Prevention technology to identify any pre-existing or new internal intrusion.



Be aware of dual-use equipment (for example, someone using a point of sale terminal for both taking money/credit card as well as normal web browsing or email activity). In general, such dual-use is frowned upon as it introduces unacceptable risk. Much safer to simply separate the functions, and keep the high risk information systems away from such high risk user activity.

Thankfully, nowadays, VLAN technology is robust, cheap, and easily implemented. Managed switches can uses untagged VLANs to implement such isolation, and tagged VLAN trunks connected to equipment such as Network Box threat protection devices to implement the policy control and Intrusion Detection / Prevention functions.

Implement

Once your high risk systems are isolated in their own network segments, it is time to design and implement the security policy for access to and from those segments.

You should ***always*** perform this from a deny everything, permit what is required, standpoint. Start by blocking all traffic into and out of these high risk networks, then identify what is required for day-to-day operation, and open up the policy to allow that specific traffic in/out. This policy needs to be as tight as possible, Here are some specific examples:

1. At the physical level, turn on ARP protection at your switch level, for those switch ports of servers and workstations connected to the high risk networks. Sure, It is slightly inconvenient when equipment is replaced/ added, but the protection against arp spoofing, combined with modern switches protection against passive network taps, is extremely effective.

2. At the firewall level, block everything then permit what is required. Connection tracking firewalls will allow you to do this with very fine grained control for most client-server network protocols today.

3. VPNs are an affective mechanism for imposing an access control layer on top of the usual network layers. But, put procedures in place to monitor VPN connections and be aware of malicious network activity bypassing firewall protections via VPNs. In general, we recommend that VPNs be terminated on the same equipment providing your policy enforcement functionality, and to subject the VPN traffic to the same policy control. VPNs should be used to increase security, not introduce backdoors to bypass protection mechanisms.

4. Assume nothing, and proxy/server locally whatever you can. For example, udp/53 traffic that looks like DNS queries can leak information – so use an internal DNS server to host these and don't permit udp/53 outbound. Same for common services such as NTP, SMTP, etc. Application identification can help tremendously with this – just because it is port tcp/25 does not mean it is SMTP traffic.

5. Look closely at web traffic requirements, and lock it down as much as you can. Do you even need web browsers on this high risk equipment? Is it possible to just maintain a list of permissible websites, and block everything else?

6. Look closely at the requirements for such applications as eMail and file transfer. Can you block usage of those completely? Restricting the number and variety of outbound paths makes it simpler for you to monitor those remaining.

7. Consider the use of tripwire systems to detect scanning or other unusual activity within the network.

Once the policy has been implemented, turn on Intrusion Detection and Prevention systems and baseline the outbound network traffic. Then, setup alerts for anything out of the usual, in particular outbound.

Depending on your network, it may be possible to implement limits on network connection output volumes (again particularly in the outbound direction). Is it reasonable for connections to be carrying large volumes of data outbound?

In general, keep this policy as tight and restrictive as you can make it, both inbound and outbound. Not too restrictive to impact your day-to-day operations or generate false alarms, but tight enough to be able to block (or at least detect and alert on) anything out of the ordinary.

Incident Response

The last step is to arrange an incident response system within your organization and your I.T. suppliers, including the Network Box SOC supporting you.

Understand the flow of incident reports, and arrange for monitoring of periodic reports from your protection systems. Make sure your escalation procedures are in place, and tightly controlled.

Summary

This four I's approach to Identification of risks, Isolation of high risk systems, Implementation of effective policy control, and Incident response, is not new. What is new is the level and sophistication of malicious activity, and the extent.

The general approach you should be taking involves identifying the high risk systems within your network, and implementing special protection, policy control, and monitoring procedures to protect such systems.

There's an old joke about a scuba diver asking a shop for the fastest fins that they sell. When asked why, he says that he is afraid of sharks. The salesman explains that he can't possibly out-swim a shark no matter how fast the fins are. The diver replies that he doesn't need to out-swim the shark – only swim faster than his buddy. Make your systems harder to penetrate than the other guy, and your attacker may just go elsewhere.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 2nd February 2016, Network Box will release our patch Tuesday set of enhancements and fixes. This month, the regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
February 2016

This month, for Network Box 5, these include:

- Support for utiliZation stats reporting to Box Office.
- Improvements to VPN status tracking (particularly for IPSEC VPNs).
- Support for SOC backup and restore of IPSEC keys and security credentials.
- Support for external host checks in Global Monitoring System (GMS).
- Improvements to GMS reporting in poor connectivity situations.
- Support for rfc822-headers section types in MIME email unpacking and analysis.
- Packet/Connection firewall rule for destination 0.0.0.0 vs directed web client.
- Enhancements to large object tickling arrangement in HTTP protocol proxies.
- Enhanced control over INPUT and OUTPUT network firewall chains.
- Miscellaneous improvements to admin web portal filtering.
- Improved support for tracking concurrent transactions in DDoS collections.
- OpenSSH: CVE-2016-0777 roaming_common vulnerabilities in OpenSSH 5.x, 6.x, and 7.x before 7.1p2.
- OpenSSH: CVE-2016-0778 roaming_common vulnerabilities in OpenSSH 5.x, 6.x, and 7.x before 7.1p2.
- OpenSSL: CVE-2015-7575 MD5 signatures in Server Key Exchange messages in TLS 1.2.
- OpenSSL: CVE-2015-3197 SSLv2 doesn't block disabled ciphers.
- OpenSSL: CVE-2016-0701 DH small subgroups.
- DHCP: CVE-2015-8605 UDP payload length not properly checked.
- Various (mostly internal) enhancements to several internal support systems.

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

Network Box ISO 9001 / ISO 20000 / ISO 27001 certified Security Operations Centre, ensures that customers' networks are protected against cyber threats, 24x7x365.

Network Box 3 Features
February 2016

On Tuesday, 2nd February 2015, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for Network Box 3, these include:

- Enhancements to Box Office and Response web sites
- Various (mostly internal) enhancements to several internal support systems

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box UK
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com

Silicon Valley Communications
Info Security Global Excellence Awards 2016

Network Box is proud to announce that the company was named as a finalist for the 12th Annual 2016 Global Excellence Awards in six categories:

- Integrated Security and Unified Threat Management (UTM)
- Managed Security Services
- Security Products and Solutions for Education
- Security Products and Solutions for Finance and Banking
- Security Products and Solutions for Healthcare
- Security Products and Solution for Small Businesses and SOHO

Winners will be honored during the annual awards ceremony which will take place in San Francisco on February 29, 2016.

link: http://www.infosecurityproductsguide.com/world/

Network Box Germany
comTeam Partnership

comTeam SYSTEMHAUS-VERBUND

Network Box Germany, started the new year by signing a partnership agreement with comTeam, to offer complete solutions in the areas of Information Technology, for Germany.

link: http://unternehmen-heute.de/news.php?newsid=330387

2016 SC Awards U.S. Finalist
Excellence Awards

Network Box has been named a Finalist, in the upcoming SC Magazine, Excellence Awards, in the following categories:

- Best UTM Security Solution
- Best SME Security Solution

Winners will be announced at the awards ceremony on March 1, 2016.

link: http://www.scmagazine.com/sc-awards-2016/section/5433/?publishDate=False&timestamp=635852806671307920