In the Boxing Ring December 2020

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

Welcome to the December 2020 edition of In the **Boxing Ring**

This month, we are talking about **Safely and Securely Working from Home**. A year into the COVID-19 pandemic, we've learned a lot about securely connecting our staff working from home. On pages 2 to 3, we recap the main concerns for remote working such as network-level threats, split-tunnel, infected workstation threats, and face-to-face verification; and discuss ways to address these problems.

Network Box's Managing Director, Michael Gazeley, was invited to speak at the University of Hong Kong's **Information Security and Personal Data Protection Awareness Week**. In this month's Media Courage, Network Box was featured in **Brilliance Security Magazine**, **RTHK Radio 3**, and the **HKEJ**. Finally, new episodes of **HPCC Hackpod Club** is now available for listening.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
December 2020

Stay Connected

You can contact us here at Network Box 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:

https://twitter.com/networkbox

https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

https://www.linkedin.com/company/network-box-corporation-limited/

https://www.youtube.com/user/NetworkBox

In this month's issue:

Page 2 to 3

Safely and Securely Working from Home

In this month's featured article, we highlight the security issues for remote working and discuss in detail, best practices and ways to address these problems.

Page 4

Network Box Highlights:

- **University of Hong Kong: Information Security and Personal Data Protection Awareness Week**
- **Network Box Media Coverage:**
  - Brilliance Security Magazine
  - RTHK Radio 3
  - HKEJ
  - HPCC Hackpod Club

NOTE: With effect from January 2020 we have switched to a quarterly Patch Tuesday cycle for Network Box 5. However, essential security fixes will continue to be released out-of-cycle, if necessary.

Safely and Securely Working from Home

A year into the COVID-19 pandemic, we've learned a lot about securely connecting our staff working from home. This month we recap the main concerns and ways we can address these problems.

Network Level Threats

To provide effective access control, we need to differentiate between our staff working outside the office, connecting over the Internet, and other Internet connections (both malicious and legitimate). We also need to protect plaintext application protocols from eavesdropping and tampering while traveling over the public Internet. Typical source IP address or network segment firewall restrictions can't do this.

The obvious solution to these problems is Virtual Private Network (VPN) technology. Of the options available, SSL (Secure Sockets Layer) VPNs are the clear winner for this type of application. Unlike more complex protocols such as IPsec (Internet Protocol Security), SSL VPNs operate over NAT (Network Address Translation) connections with just a single TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) port required to be opened.

They use the same encryption technologies as those used by your online bank. Authentication is best implemented at several levels:

Base network packet level

Using a TLS key and providing a very simple authentication key shared amongst all users effectively differentiates US from THEM, and protects against Denial of Service and other style attacks.

SSL certificates, authenticating the machines

Typically, both client and server-side certificates are used, so both ends of the connection can identify and authenticate each other.

User authentication

Using the traditional ***username+password*** method, user authentication securely identifies the user at the client-side of the connection (the worker at home). You can typically connect this to your central authentication system to avoid maintaining and controlling separate passwords.

Dual Factor Authentication

Running on top of user authentication can supplement the ***'something I know'*** of username+password with a ***'something I have'*** dual-factor authentication token. This process can vastly improve the security of the user authentication mechanism. Unlike a rarely changed password, dual-factor tokens typically change each time they are used or every 30 seconds.

Once the VPN connection has been established, the user, the user's workstation, and the VPN gateway that the user is connected to, are all authenticated. Any traffic passing through VPN is securely encrypted against eavesdropping, and protected against tampering and replay style attacks. Unlike web gateway style SSL systems, true SSL VPNs connect at the layer 3 network level - enabling both source IP and network segment based access control.

Split-Tunnels

While split-tunnel technology (where traffic destined for the office systems is directed through the VPN, but other general traffic goes to/from the Internet directly) is available, Network Box Security Response does not recommend this approach.

With today's high-speed Internet connectivity, it is generally safer to direct ALL traffic through the VPN tunnel. This way, the same gateway-based protection systems and policies available to workers in the office can be applied to workers connecting from home or on the road:

- The same anti-malware
- The same URL content filtering policies
- The same firewall policies and controls

The Infected Workstation Threat

It is good practice to impose the same policies and restrictions on remote workstations as for those workstations in the office. That usually means providing remote workers with a dedicated laptop for office connections. The extra costs involved are generally far less than the costs of a security breach/incident from a less protected workstation, and worker satisfaction is higher.

With VPN connections made at the network level, the same tools and procedures for automated management, application deployment, and updates, can be applied as for office workstations. Just beware that network bandwidth may be limited and latency greater. Keeping applications local or using thin client web-based applications can help with this.

Face to Face Verification

When working in the office, we are used to having face-to-face meetings. Instructions are often verbal and easily verified. There is also something inherently 'human' about seeing someone's face and talking to them directly that can never be replicated over email or text messaging. Think about how often you see rude or unacceptable comments/behavior behind online communications' anonymity versus the last time someone was rude/unacceptable to your face.

However, we do need to be concerned with how that lack of face-to-face contact affects our security. It is far easier to impersonate someone online than in person.

One solution is to use authenticated communications (in particular for financial or otherwise sensitive messages). Email is notoriously insecure and trivial to impersonate someone, but security can be strengthened using digital signatures. While complex to set up and often hard for users to understand, PGP/GnuPG (Pretty Good Privacy/GNU Privacy Guard) and SSL certificates offer two ways of doing this for more sophisticated users.

An alternative is implementing an alternative verification mechanism using natively secure messaging systems such as telephone calls, instant messaging (WhatsApp, line, etc.), or video calls. Make sure the procedures are in place to verify all potentially damaging instructions via a different mechanism to that in which the instructions are first received. In this way, you can protect yourself against phishing and other fraudulent financial attacks.

Building on SSL VPN's core technology, you can safely and securely integrate remote workstations and workers into your office and data centre systems. Plan for the worst, and make sure that you have disaster recovery systems in place to facilitate business continuity and working from home, even if your workers are currently in the office.

Video conferencing systems are now easy to deploy, cost-effective, and widely available - Skype, GoToMeeting, Zoom, Microsoft Teams, WhatsApp, etc. No matter the technology, encourage and facilitate their use within your organization. They can help bring local and remote workers together, improving their social interactions and greater security.

Bandwidth is cheap vs. the costs of your organizational compromise.

Network Box HIGHLIGHTS

Network Box Hong Kong

University of Hong Kong - Information Security and Personal Data Protection Awareness Week

Network Box Managing Director, Michael Gazeley, was invited to speak at the University of Hong Kong's **Information Security and Personal Data Protection Awareness Week**. The seminar was titled, "Managing your Cyber Risk for Remote Working," and took place at the Meng Wah Complex, which coincidently, was donated to the university by Michael's grandparents.

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
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

Network Box Media Coverage

Brilliance Security Magazine

Virtual Patching

LINK: https://bit.ly/3nYS29S

RTHK Radio 3

Backchat with Hugh Chiverton

Children as victims in Internet sex crimes

LINK: https://bit.ly/364XIsz

HKEJ

The healthcare industry has become a prime target for hackers and cybercriminals

LINK: https://bit.ly/2V2XAUf

HPCC Hackpod Club

- **Episode #5: News from the hacker scene**
- **Special Report: IT start-up in Corona times**

LINK: https://bit.ly/364w0wi