

In the Boxing Ring OCT 2019



Network Box Technical News

from **Mark Webb-Johnson**

Chief Technology Officer, Network Box

Welcome to the October 2019 edition of In the **Boxing Ring**

To kick off **Cybersecurity Awareness Month**, Network Box's Managing Director, Michael Gazeley, will be talking about **5 Key Cybersecurity Suggestions for IT Managers**. During this month, one can expect a deluge of sensible cybersecurity advice, however, typical examples have mostly been focused on end-users. As Network Box is a Managed Security Service Provider for organizations, it would be more relevant for us to provide cybersecurity advice for IT Managers instead. On pages 2 to 3 we go through our five suggestions.

On page 4, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

In other news, Network Box Hong Kong participated in Macquarie Group's **Cybersecurity Awareness Week**, to talk about the Dark Web. In addition, Network Box Germany took part in the **Server-Eye Partner Day**. And in this month's Media Coverage, Network Box Hong Kong was interviewed by the **Financial Times** and the **South China Morning Post**; Network Box USA was featured in **SC Magazine**; and **it.daily.net** interviewed Network Box Germany to talk about the new S-80i hardware platform.



Mark Webb-Johnson

CTO, Network Box Corporation Ltd.
October 2019

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

Cybersecurity Awareness Month: 5 Key Suggestions for IT Managers

October is Cybersecurity Awareness Month. Originally established in collaboration between the U.S. Department of Homeland Security and the National Cyber Security Alliance to raise awareness in an increasingly digital world. In light of this, on pages 2 to 3, we discuss our five key cybersecurity suggestions for IT Managers.

Page 4

Network Box 5 Features

The features and fixes to be released in this month's patch Tuesday for Network Box 5.

Page 5

Network Box Highlights:

- **Network Box Hong Kong**
Macquarie - Cybersecurity Awareness Week
- **Network Box Germany**
Server-Eye Partner Day
- **Network Box Media Coverage**
 - Financial Times
 - SCMP
 - SC Magazine
 - it.daily.net



Cybersecurity Awareness Month

5 Key Suggestions for IT Managers

by **Michael Gazeley**
Managing Director
Network Box

October is Cybersecurity Awareness Month. Originally established in collaboration between the U.S. Department of Homeland Security and the National Cyber Security Alliance in 2003, this annual event has successfully evolved to become an important reminder, of the critical nature of cybersecurity in an increasingly digital world.

During October, everyone can expect a deluge of sensible cybersecurity advice. Typical examples are for end-users, such as:

- Review the privacy settings on your social media accounts
- Ensure you don't fall for email phishing scams
- Always backup your data to at least three different kinds of media, one of which should be offsite
- Keep your operating system and applications up-to-date
- Don't click on a link, unless you are very confident where it's from.

And so on.

As Network Box is a Managed Security Service Provider for organizations, however, let's look at 5 key cybersecurity advice for IT Managers instead.



1. Update Your Systems In Real-time

Always make sure your cyber-security systems are as up-to-date as possible. That doesn't mean being up-to-date within a day or two, that means being up-to-date within SECONDS of updates being available. Network Box's patented PUSH update technology, helps to ensure every online Network Box system in the world, is updated within 45 seconds of new patches or signatures being issued.

Augmenting PUSH, is Network Box's zero-day cloud, based anti-malware defence shield, Z-Scan. The award winning engine mitigates new threats within 3 seconds (on average) of being sampled in the cloud. Behavioural analysis, sandboxing technology, and other real-time testing of unknown threats is all very well, but there is nothing better than having the exact preventative signature in place BEFORE a zero-day threat arrives at your organization's Internet gateway, which Z-Scan provides.

2. Lock Down Your Technology

Be very aware that many cybersecurity products and services include back-doors. An educated guess, leads one to conclude that such back-doors are inserted by governments; which means that when governments themselves get hacked, they lose the keys to these backdoors to cyber-criminals. If that sounds farfetched, know that one of the most successful ransomware attacks in history, WannaCry, was built on EternalBlue, a cyberattack exploit developed by the U.S. National Security Agency (NSA).

Network Box is extremely proud to be able to say, we have no secret backdoors in any of our products or systems. Always install cybersecurity without unauthorized backdoors, and ask potential vendors point-blank to guarantee they have never been found to have included a backdoor in any of their systems or services.

3. Monitor The Dark Web

Sign up for a Dark Web Monitoring service, so that you know, if and when, your End-Users have had their credentials compromised. This is critical, because on average 30% of people use the same password everywhere. That means a hacker may not even need to hack your system to get in; they can just search for your domain on the Dark Web, and try to use the names and passwords which they find there.

By monitoring the Dark Web, an IT Manager can stay one step ahead of leaked passwords, hoax blackmail attempts, and sophisticated Identity Theft. And in the unfortunate event their own network system actually gets hacked, Dark Web Monitoring could be the first reporting tool to discover the data breach. In many countries around the world, it is now a legal requirement to report data breaches.

4. Scan Encrypted Traffic

The majority of websites now use HTTPS (Hyper Text Transfer Protocol Secure), which is a secure protocol for communication between systems, such as a web browser and a web server. It is therefore **absolutely critical** that HTTPS traffic is scanned for threats.

Far too many organizations still only scan unencrypted HTTP web traffic, while leaving HTTPS web traffic unscanned. The reality is that in order to scan HTTPS / SSL encrypted traffic, it is necessary to install a Trust Certificate on each device on the network. This does take some time and effort, (although there are various enterprise tools to ease this task), but we are normally only talking about a few seconds per device. The alternative outcome for not implementing this? Your entire network could be successfully attacked by ransomware or other exploits, ultimately sending your whole organization back to the stone age.



5. Leverage a SIEM System

Any IT Manager trying to monitor, manage, and report, on their network's cybersecurity in real-time, has their hands absolutely full. Multiply that effort by multiple networks, add-in the need for PCI DSS (Payment Card Industry Data Security Standard) compliance; and you realize the superhuman effort which would be required to carry out this work on a 24x7x365 basis. The need for an automated response becomes crystal clear.

By leveraging the NBSIEM+ (Network Box Security Incident and Management Plus) system, it is possible to provide real-time monitoring and analysis of security alerts, which are generated by both applications and network hardware, including routers, switches, and firewalls.

If you are already a Network Box client, please contact your local Security Operation Centre to discuss these issues, and more. If not, then you are still more than welcome to give us a call, to see what we can do for you. In the end, you either become a planner, or you become a victim. It's cybersecurity awareness month – don't become a victim.

Network Box



NEXT GENERATION MANAGED SECURITY

On Tuesday, 1st October 2019, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOC's will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features October 2019

This month, for Network Box 5, these include:

- Improvements to HTTP protocol support in web proxies
- Support ICMP ping check for GMS external hosts
- Support configurable source address for GMS external host checks
- Additional support for new regional Security Operation Centre public address ranges
- NBSIEM+ support for per-asset configuration of data inject and cold storage options
- NBSIEM+ support for hot and cold storage accounting
- Performance and stability improvements to Box Office Notifications
- Improvements to tracking and reporting of device status
- Enhanced GMS monitoring of signature status



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 HIGHLIGHTS



Network Box Hong Kong Macquarie Group - Cybersecurity Awareness Week



Network Box Hong Kong took part in Macquarie's Cybersecurity Awareness Week, conducting a seminar on the Dark Web, the dark side of the Internet. Various topics were covered, not least the threats posed by the Dark Web in terms of Identity Theft, Data Theft, and Credential Theft. In particular, credential theft, can lead to the serious compromise of workplace security, because approximately one third of people globally, use the same passwords for multiple accounts.



Network Box Germany Server-Eye Partner Day

Network Box Germany was at the Server-Eye Partner Day held in Saarbrücken, to talk about Managed Security Services and highlight key Network Box 5 security technologies.



Network Box Media Coverage



Financial Times
HKEX blames software bug for outage as website comes under attack
LINK: <https://on.ft.com/2kKKgp6>



SCMP
Beleaguered Hong Kong hit by double whammy as Fitch Ratings downgrades city and stock exchange hit by cyberattacks
LINK: <https://bit.ly/2mJj62y>



SC Magazine
Warner presses CBP on security best practices for third-party contractors
LINK: <https://bit.ly/2lfaiAV>



it-daily.net
Network Box Extends Its S-Series
LINK: <https://bit.ly/2mCczqa>

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