In the Boxing Ring
MAY 2023

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the May 2023 edition of In the **Boxing Ring**

This month, we are talking about **Configuration Reviews.** Most security frameworks include periodic configuration reviews as a core requirement. Whilst all configurations should adhere to the defined security policy at initial deployment, and all subsequent changes should have been made in accordance with that policy, this is often insufficient. As part of the general move towards Managed Detection and Response, Network Box SOCs have recently begun conducting formal configuration reviews. On pages 2 to 3, we discuss this in detail.

In other news, Network Box Hong Kong was at the **InnoEX 2023** – Physical Fair, which took place at the HK Convention and Exhibition Centre. During the four-day expo, Network Box Managing Director, Michael Gazeley, gave a talk titled: ***The top 10 cybersecurity facts you need to know.*** And in this month's global security headlines, there were security issues with Intel CPUs, Schneider Electric, Cisco, macOS, Windows, Hyundai, and Western Digital.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
May 2023

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:

Configuration Reviews

Most security frameworks include periodic configuration reviews as a core requirement. Whilst all configurations should adhere to the defined security policy at initial deployment, and all subsequent changes should have been made in accordance with that policy, this is often insufficient.

For example:

1. Individual configuration changes may impact other configuration items in unexpected ways (such as a network addressing/routing change exposing firewall rules to new traffic).
2. Policies and risk tolerance may change so that what was acceptable in the past may no longer be acceptable today (such as new threats, vulnerabilities, and attack vectors).
3. Staff may leave, and with them, the knowledge of mitigations previously put in place (such as the reason for a particular service to be exposed and steps taken to mitigate that risk).

Network Box has always followed the approach that the customer sets the policy, and the SOC securely implements that policy in the configuration. We are frequently asked to recommend policies or to suggest optimal deployment approaches, but the policy itself is entirely under the control of our customers.

A year ago, we formalized our general security recommendations by introducing a set of best practices (**https://network-box.com/best-practices**); developed over two decades of delivering Managed Security Services, investigating security incidents, and working with our customers to protect their networks. These Best Practices represent the most common forms of network infiltration and data breaches that we see affecting networks worldwide. Many of these best practices can also be found in common standardized security frameworks. Our Security Engineers refer to these Best Practices when designing defense systems for networks under management when processing policy change requests, and during periodic configuration reviews. While ultimately, the customer decides the policy; we strive to inform, warn, and point out when policies conflict and open up networks to common attack vectors and unnecessary risk.

As part of the general move towards Managed Detection and Response, Network Box SOCs have recently begun conducting ***formal configuration reviews*** with reference to these best practices. You will see the results of these reviews as PDF reports attached to tickets raised in Box Office / NBSIEM+. The initial review will highlight all areas of concern, and subsequent reviews will also include a table of changes (additions, changes, and resolved concerns) since the previous review.

We encourage you to work with our Security Operation Centres to address highlighted items and to use this system to improve your security policy and defense.

Network Box HIGHLIGHTS

Network Box Hong Kong
InnoEX 2023

Network Box Hong Kong was at the **InnoEX 2023** – Physical Fair, which took place at the HK Convention and Exhibition Centre. During the four-day expo, visitors were introduced to Network Box's award-winning security technologies and managed services. Additionally, Network Box Managing Director, Michael Gazeley, gave a talk titled: ***The top 10 cybersecurity facts you need to know.***

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

Global Security Headlines

Bleeping Computer
Intel CPUs vulnerable to new transient execution side-channel attack
LINK: https://bit.ly/3VbqXC5

SC Magazine
Schneider Electric issues patches for 3 vulnerabilities in APC UPS units
LINK: https://bit.ly/3oKRg5X

Bleeping Computer
Cisco discloses XSS zero-day flaw in server management tool
LINK: https://bit.ly/3VdVAGY

Cyber Security News
First-Ever Ransomware Found to be Attacking macOS
LINK: https://bit.ly/41QUqDR

Bleeping Computer
Windows zero-day vulnerability exploited in ransomware attacks
LINK: https://bit.ly/44a20ek

iTech Post
Hyundai Car Owners in France and Italy Affected by Data Breach
LINK: https://bit.ly/3Li4VZW

Yahoo! Finance
Western Digital Data Breach: Hackers Demand Huge Ransom in Exchange of Sensitive Data
LINK: https://yhoo.it/3nesUkw