MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

FOR COMCEN/SIG USE

PRECEDENCE ACTION/PRECEDENCE INFO
"PRIORITY"

FM: CG, PA

TO: All Unit Commanders
Attn: G6/Signal Officer/IS Officer

INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA

GROUP:
14 January 2016

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 1401-35-2016

INFO: CSAFP
Attn: J6

1. References:

   a. Command Guidance
   b. VAPT and PANET Monitoring Result

2. As per above references, forwarded is the Cybersecurity Bulletin number 042 with topic regarding **Top Must-Know Network Security Tricks.**

3. ITR, all concerned G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cybersecurity Awareness of the Philippine Army.

4. For information and widest dissemination.

DRAFTER'S NAME AND TITLE MAJ JOEY T FONTIVEROS (INF) PA Chief, CMB, OG6, PA	**PHONE NR:** 6630
RELEASER'S NAME AND TITLE COL VENER ODILON D MARIANO GSC (SC) PA AC OF S FOR CEIS, G6, PA	

HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB

14 January 2016

CYBER SECURITY BULLETIN

Cyber Security Bulletin: #42

TOP MUST-KNOW NETWORK SECURITY TRICKS

Network security is one thing all Network Administrators agree will keep them up at night. For new network administrators and database administrators, there are a few security tricks that can keep your infrastructure safe from attacks and malicious behavior. Below are tips and recommendations from industry experts who know the importance of securing your network from internal and external intrusions.

Create Unique Infrastructure Passwords

"One of the most common mistakes made in network security is to implement a shared password across all routers, switches, and infrastructure devices. The compromise of one device or leakage of the password can lead to a compromise of every device - not only by an insider, but also by malware that targets these devices. As a best practice security recommendation, each device should have a unique password in order to limit the liability of the device being leveraged against its peers."

-Morey Haber, VP of Security, BeyondTrust

Use Scheduled and Event Based Password Changes

"While the management of network passwords has become commonplace with a variety password management tools, the changing of passwords on a large scale generally requires a dedicated 'password safe' tool. Manually changing passwords for hundreds or thousands of devices is labor intensive and generally avoided by organizations because of time constraints, unless a dedicated tool is procured. As per regulatory compliance initiatives and security best practices, passwords should always be rotated on a periodic basis, making this exercise rather problematic. In addition, based on events, ad-hoc changes may need to occur to passwords based on employment changes and events like contractor access.

"Therefore, it is recommended to use a schedule to change all of your network passwords on a regular basis, or have a process to change them ad-hoc if needed, and if the time required to make these changes is excessive, consider a solution to automate the process."

-Morey Haber, VP of Security, BeyondTrust

Harden the Devices from Default Settings

"Almost every device has default settings and passwords when it is first installed. It is up to the end user to change account names, passwords, secure ports, and harden the device from malicious activity.

"As a best practice for network security, it is recommended to change all these settings, and to also use a tool to assess whether the devices are properly hardened, do not contain default passwords for things like SNMP (Simple Network Management Protocol), and are running the latest firmware to vet out any vulnerabilities and missing security patches. Unfortunately, many organizations install devices and do not actively place them into a device management life cycle for patching, configuration, and maintenance to keep them secure like servers or workstations."

-Morey Haber, VP of Security, BeyondTrust

Set Up a Dedicated Network for Business-Critical servers

"Segregating business critical servers and systems to their own network or subnetwork can often be very beneficial. By placing these systems in their own network you maximize their connection quality and decrease their network latency by limiting the amount of non-critical traffic near them. Additionally, you gain the security of logically separating the packets around your most important systems allowing you to better monitor and shape the network traffic."

-Neil Marr, Director of IT, LearnForce Partners LLC, ExamForce

Always Log and Study Suspicious Activity

"Deny all outbound network traffic not specifically allowed **and log it**. Then look at it. The log data will provide an enormous amount of information about what is happening, both good and bad, on your network."

-Brian O'Hara, Senior Security Consultant, Rook Security

Never Use Default Security Settings On Internet Devices

"Make sure you have hardened any internet facing device and change the Admin username and password to something fairly hard to crack!"

-Brian O'Hara, Senior Security Consultant, Rook Security

Be Picky About Your Traffic

"Only allow specific, required traffic both inbound and outbound on your network. If an application and/or associated port is not needed, block it. This takes some time and tuning but is well worth the effort."

-Brian O'Hara, Senior Security Consultant, Rook Security

Block IP Ranges From Suspicious Foreign Bodies

"Unless you do business in China, Russia, North Korea, etc. **block their IP ranges**. It will not stop those that are really interested in getting to your facilities but it will stop a lot of 'browsing around' to see what you have."

-Brian O'Hara, Senior Security Consultant, Rook Security

Break the Addiction

"Assume your user base is compromised and break your addiction to big data analytics in your security program. Today, most security strategies focus on protecting everything - including the user host. This creates volumes of data that burdens artificial intelligence."

"Assume your user base is compromised and focus your security efforts in anomaly detection between users, applications and the database. Some may dispute that this is possible, but the banking industry has achieved this with their customer base. Enterprises can mirror this approach with success."

-Jeff Schilling, Chief Security Officer, Armor

Elevate & Control

"Implement permission access management (PAM) controls that only authorize elevated privileged access for a short time. Most APTs (Advanced Persistent Threat) are successful because they obtain elevated privileges, which they keep indefinitely. This allows threat actors to holster their arsenal of malicious tools and "live off the land" as an authorized user with elevated privileges.

"There are many PAM solutions that allow organizations to manage elevated, time-based privileges. Some may even be mapped back to a trouble ticket. This breaks the cyber kill chain for threat actors and stops them from being persistent."

-Jeff Schilling, Chief Security Officer, Armor

DO YOU WANT TO KNOW MORE? TALK TO US.

POCs:

a. **MAJ JOEY T FONTIVEROS (INF) PA** – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-628-1057.

b. **Sgt Mark Dave M Tacadena (SC) PA** – Branch NCO, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0998-534-2877

.Reference:

This was cross-posted from https://www.techopedia.com/2/31554/security

/top-must-know-network-security-tricks.