Army Vision: By 2028, a world-class Army that is a source of national pride.

H E A D Q U A R T E R S
P H I L I P P I N E A R M Y
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR
COMMAND AND CONTROL COMMUNICATIONS, AND CYBER SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB 13 January 2017

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #17-02

INSIDER THREATS

If we fail to consider insider threats in cybersecurity (rather than dismissing everything as human error), we can cover the different types of human error. No matter how we look at it, the military can no longer afford to suffer such high volumes of insider threats on an annual basis.

3 Types of Insider Threats in Cybersecurity

The high-profile data breaches in the news are more likely that they were carried out by outside attackers. However, attackers are moving from primitive brutish means to a future of more finesse and stealthy threats, taking advantage of security vulnerabilities created by their own employees.

When you think about how these insiders create such dangerous vulnerabilities, there are 3 main types of threats to be concerned with:

1. Accidental: According to Verizon's 2016 Data Breach Incident Report, accidents accounted for 30% of security incidents in 2015. In this case, our personnel might just not be educated enough on cybersecurity best practices. Whether insiders open a phishing email or click on a malicious link, attackers are just waiting for our personnel to slip up.

2. Negligent: These are the inside threats where our personnel try to avoid the policies we've put in place to protect endpoints and valuable data. For example, if we have strict policies for external file sharing, personnel might try to share work on public cloud applications so they can work at home or at the barracks. There's nothing wrong in these acts, but they can open our network up to dangerous threats nonetheless.

3. Malicious: This type of insider threat is often overlooked because we rather look at malicious intent from third-party actors. However, there are times when personnel within the military organization are motivated by financial gain or espionage to make us vulnerable. For example, a disgruntled soldier who was recently discharged or reassigned might extract sensitive data on his/her way out and either sell it or release it publicly.

It's difficult to find concrete data regarding accidental or negligent insider threats because they don't often result in a security catastrophe. Sure, there are instances in which an accidental vulnerability leads to an attacker's gain, but attacks have become such an inevitability that even small incidents can be overlooked at times.

Negligent and accidental insider threats can often be mitigated by more effective and accessible security policies that also avoid being too invasive for personnel. Malicious insider threats, on the other hand, are a rising challenge that the Philippine Army must be prepared to overcome.

Are Our Personnel Being Recruited by Cyber Criminals?

The dark web market for stolen credit card and personally identifiable information (PII) is massive, with some estimates claiming its worth around $120 billion. While the values of different types of data vary, the fact remains that cyber criminals stand to see financial windfalls if they can capture sensitive information.

One way cyber criminals are starting to collect sensitive data is to recruit our personnel and turn them into malicious insider threats. A recent McAfee report specifically cites the healthcare industry as one that is plagued by this kind of insider threat.

Unlike accidental and negligent insider threats that could be mitigated by, for example, more diligent patching practices, these malicious insider threats must be monitored more carefully.

So how do you actually protect your company from malicious insider threats? According to Verizon's 2016 DBIR, it's all about relentless monitoring of employee daily activity (especially if they have privileged accounts) and understanding where your sensitive data resides.

Reference:

This was cross posted from:
http://www.csoonline.com/article/3149754/security/insider-threats-in-cyber-security-more-than-just-human-error.html

DO YOU WANT TO KNOW MORE? TALK TO US.

POC: LTC JOEY T FONTIVEROS (SC) PA – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-6281057. Email: fontiverosjt@army.mil.ph.