James Everett Tourtellotte IV
ITN 266
Professor McLaughlin
1/28/2023

The first article I read was found on the following link: https://www.theregister.com/2023/01/24/ukraine_nato_cyber_defense/ . This article outlines how Ukraine has made a formalized agreement to participate in the security alliance titled “Joint Center for Advanced Technologies in Cyber Defense” (CCDCOE). It further explains how this organization is a knowledge hub, research institution, and training facility for cyber-defense. This is of course relevant to world events as Ukraine has been the victim of pretty hefty cyber attacks since early 2022. A common principle that I have learned studying cybersecurity is that “sharing is caring”. Cybersecurity is an ever developing field that requires as many bright minds as humanly possible. When we come together, we only strengthen ourselves. It is common practice for professionals to share their research, and/or team up for the better of their institutions. This is outlined here as it is stating that Ukraine is joining an alliance of sorts. I personally believe this will help their entire security posture as they likely have access to resources that were not there in the first place. A screenshot of the article is below:

SIGN IN / UP

The Register

GOVERNMENT TECH WEEK

59

Ukraine slides closer to NATO with buckets of experience fending off Moscow's cyberattacks

'Now Russia will have to play defense'

Jessica Lyons Hardcastle

Tue 24 Jan 2023 // 08:25 UTC

Ukraine has taken another step toward deepening its ties to NATO by signing an agreement to formalize its participation in the security alliance's Joint Center for Advanced Technologies in Cyber Defense (CCDCOE).

The CCDCOE functions as a cyber-defense knowledge hub, research institution, and training and exercise facility that assists members with technology, threat-sharing and policy expertise. CCDCOE membership is not limited to NATO nations.

Ukraine submitted its application to join the Estonia-based center in August 2021. Last April, the 27 sponsoring nations in the steering committee unanimously endorsed Ukraine as a contributing participant in the CCDCOE — thus giving the other member state's access to Ukraine's "valuable first-hand knowledge of several adversaries".

That language was a nod to both the cyberwarfare tactics Russia employed ahead of and during its illegal invasion of Ukraine, and Moscow's earlier attacks against Ukraine's power grids and other digital targets.

The newer technical agreement, which must be signed by all of the center's member countries, would formalize Ukraine's participation in the cyber-defense group.

"During the past year, we already actively cooperated with the United Center of Advanced Technologies for Cyber Defense of NATO," Ukraine's Yuriy Shchygol, head of state special forces, said in a statement.

Indeed, Shchygol's country has been ground zero for countering Russian cyberattacks. The Computer Emergency Response Team of Ukraine (CERT-UA) tracked 2,100 incidents and cyberattacks last year alone, and more than 1,500 of those occurred after Russia's full-scale military invasion in February.

The CCDCOE director and its international relations chief visited Ukraine in November 2022 to discuss its experience countering Russian cyberattacks. "I hope that our cooperation will only strengthen this year," Shchygol added.

The Register asked the center's Baltic member states for comment and did not immediately receive any response.

The second article from eweek.com was titled “How to Guard Against the Biggest Cloud Security Threats and was found on the following link: https://www.eweek.com/cloud/cloud-security-threat/ . The article goes over a couple errors in Cloud Security and a few protective measures against cloud threats. The two errors discussed were Lack of Training and what can be defined as “hyper progress”. It discusses how much of the cloud is configured by people, and that improperly trained individuals can pose an inadvertent risk to a company by being ill-prepared for the job.

The second problem revolved around the idea that Cloud Providers are moving to fast. This amount of progress has left certain customers exposed as they become out of the loop due to the advancement speed and lack of human resources. For example, it described a customer that was automatically opted out of encryption until an agreement was read and accepted. This ended up leaving the customer vulnerable to a data breach. The article states that you can fix these human based issues with more human based remedies.

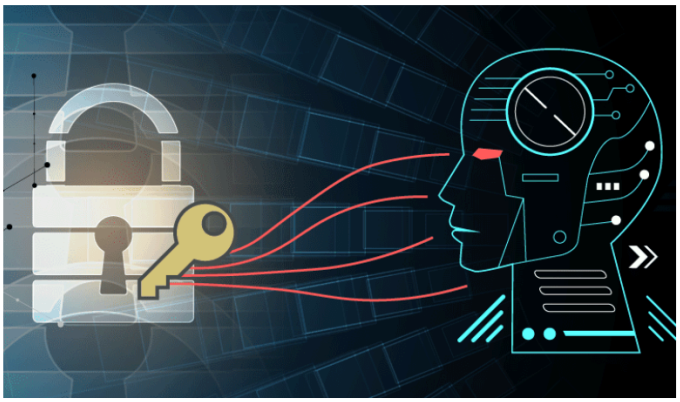
For example a solution was peer-approved configurations. This I agree with. I see nothing wrong with having a hierarchy of skill sets in a workplace. The second one, less human involvement, was Automated Checking and Testing. This is a great remedy for Cloud Providers. If there is the equivalent of Nessus, but for Cloud Providers, I would say they should integrate that into their security posture. Automatic updates are a great security measure. Below is a screenshot of the article:

Cloud Cybersecurity

How to Guard Against the Biggest Cloud Security Threats

Human mistakes made by your staff remain a huge cloud security risk. Train your staff to protect the enterprise against themselves.

By **David Linthicum** - June 2, 2022



IBM recently announced the results of a global study which found that data breaches in 2021 cost the companies studied $4.24 million per incident on average. For those of you keeping track, this is the highest cost in the 17-year history of the report.

Are these hoody-wearing bad-actors sitting in some evil country, working overtime to hack our system walls and breach our data? In many cases, the employees sitting down the hall inadvertently leave the doors wide open to breaches.

Most of the scenarios that allow data breaches to occur are simple misconfigurations or human error. This happens when a security administrator or end user fails to properly set up certain security attributes. Thus, access to a compute or storage server in the cloud is left wide open and vulnerable to a breach – without any special talent required to rupture security.

In a recent report, McAfee connected the rise of cloud breaches and the state of multi-cloud adoption. Their report found that, in recent years, nearly 70 percent of exposed records—5.4 billion total—were caused by unintentional Internet exposure due to misconfigured cloud services.

Even more alarming, McAfee found that most of these misconfigurations go unreported and, in many cases, unnoticed. This gets us to the heart of the matter, in that it's humans doing something stupid that easily enables bad actors. What's more, when the mistakes are found, they are often ignored or covered up because of the bad PR it would cause, or to avoid employee disciplinary actions.

Also see: The Successful CISO: How to Build Stakeholder Trust

Causes of Human Errors in Cloud Security

So, what mistakes do humans make when they set up their cloud security? While there are any number of reasons for the errors, here are the two most common:

The last article I read was about the recent Hive Ransomware attacks that had occurred in the past 2 years. It can be found using the following link: https://thehackernews.com/2023/01/hive-ransomware-infrastructure-seized.html . The article outlines how the DoJ and FBI covertly infiltrated the Hive database servers and captured 336 decryption keys that were then handed over to companies who had been compromised by Hive. This apparently saved around roughly $130 million in ransomware payments. There is not much more to the article other than some of the ways Hive did what they did, and recklessly stating how the FBI and DoJ attained knowledge about the Hive group. This brings me to my opinion on the article: I have mixed feelings about it.

Have you ever heard a Navy Seal on a Podcast? Take the entire population of Podcasts with Navy Seals, and the majority of those Podcasts will have a moment where the Navy Seal would go “I just wish people would stop talking about what the Navy Seals do.”. Most of this attitude stems from the idea that the more you publicize what you’re doing as an operator, the harder you could make engagements in the future. Personally, whoever gave out the information that stated how they got to Hive’s database server should be told to not do that in the future. The surviving members of Hive are most certainly going to use this “loss” as a way to bolster their defenses if they reform. They would likely do what we feared the Germans could do if they knew about the Enigma project before it was used - bolster their defenses. Given that it was already so difficult to get the decryption keys, and they did not even capture a human being - I see the Public Relations attempt that appears obvious here as a loss.

At the end of the day, the companies that were victims to this attack were likely victims because of their own poor security posture - that can easily be fixed with money that companies definitely have. Those companies are not to be seen as victims. Their ignorance makes them playgrounds for malicious actors. Then when they get caught crying with their pants down - the Government “helps” the corporations. That in itself becomes another playground for these hackers to train their Evasion techniques. They will continue to do what they do, until businesses as a whole pick up the slack and integrate cyber professionals as critical assets in their business plan.

On the other hand, the progress made is still progress. I am glad to hear that the government was able to find and retrieve decryption keys, to me that is progress - a hack back. I do not know if that outweighs the details revealed in the article but I believe it to be a good thing. Below is a screenshot of the article discussed:

Hive Ransomware Infrastructure Seized in Joint International Law Enforcement Effort

Jan 26, 2023 Ravie Lakshmanan Encryption / Ransomware

In what's a case of hacking the hackers, the darknet infrastructure associated with the Hive ransomware-as-a-service (RaaS) operation has been seized as part of a coordinated law enforcement effort involving 13 countries.

"Law enforcement identified the decryption keys and shared them with many of the victims, helping them regain access to their data without paying the cybercriminals," Europol said in a statement.

The U.S. Department of Justice (DoJ) said the Federal Bureau of Investigation (FBI) covertly infiltrated the Hive database servers in July 2022 and captured 336 decryption keys that were then handed over to companies compromised by the gang, effectively saving $130 million in ransom payments.

The FBI also distributed more than 1,000 additional decryption keys to previous Hive victims, the DoJ noted, stating the agency gained access to two dedicated servers and one virtual private server at a hosting provider in California that were leased using three email addresses belonging to Hive members.

Aside from the decryption keys, an examination of the data from the servers revealed information about 250 affiliates, who are parties recruited by the malware developers to identify and deploy the file-encrypting payload against victims in exchange for a cut of each successful ransom payment.

Trending News Stories


Researchers Release PoC Exploit for Windows CryptoAPI Bug Discovered by NSA

Emotet Malware Makes a Comeback with New Evasion Techniques


Over 4,500 WordPress Sites Hacked to Redirect Visitors to Sketchy Ad Pages


Chinese Hackers Utilize Golang Malware in DragonSpark Attacks to Evade Detection

Contributed Reports

How to improve application security with Pentesting-as-a-Service

Download: The Definitive Browser Security Checklist