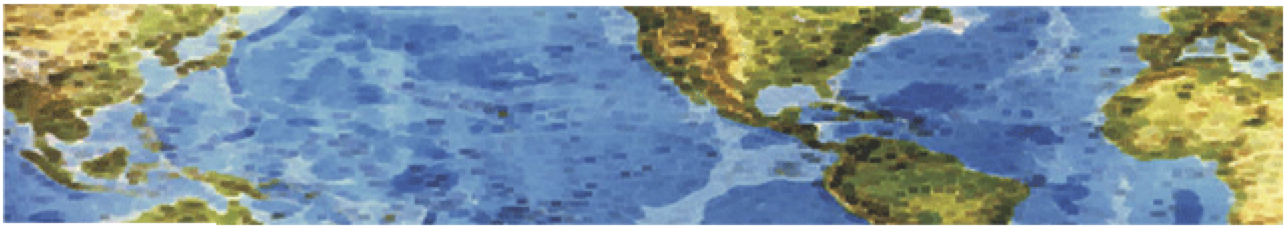
HALL ASSOCIATES



Risk-Based Decision Making Commentary
20 June 2014 Newsletter

Pentagon: Missile defenses vulnerable to cyber attack

The director of the Pentagon's Missile Defense Agency told Congress last week that U.S. missile defenses are vulnerable to cyber attacks that could disrupt its sophisticated networks of sensors and guidance systems used in targeting enemy missiles. During a Senate defense appropriations subcommittee hearing June 11, Sen. Jack Reed, (D-RI) asked MDA Director Vice Adm. James Syring how vulnerable are the communications links between radar, satellites and other sensors to cyber attacks.

"How vulnerable are those external sources to cyber attack so that someone contemplating a launch would first conduct a cyber-interruption of your guidance systems?" Reed asked. "Sir, we've looked at that. I'd like to take that to a classified session," Syring said. "It's a serious concern?" Reed asked. "Yes, sir," Syring replied.

Earlier, Lt. Gen. David Mann, commander of the Army Space and Missile Defense Command, said of potential cyber attacks: "what we're looking at internally is in terms of cyber and what can we do to make sure that we, first, identify vulnerabilities, but also put in place our ability to put up that shield, that wall" against cyber attacks. Mann said the military is also looking at the security of strategic offensive ballistic missiles that are known to be a target of nation-state cyber targeting from China and Russia. "We're looking at that very, very hard, a lot of red-teaming going on," Mann said. "And I think you know that there's a lot of countries out there that are continuously, on a daily basis, trying to access different networks." Mann added that "we're continuously looking at our different architectures and what needs to be done to harden them against cyber, because I think that's — quite frankly, that's the biggest threat that we have right now to our systems, is the impact of cyber."

http://flashcritic.com/pentagon-missile-defenses-vulnerable-cyber-attack/

P.F. Chang's Breach: Predates Target?

A handful of U.S. card issuers on June 18 confirmed Visa had issued alerts that suggested fallout from the P.F. Chang's China Bistro breach could be more far-reaching than initially suspected. Now it's believed the P.F. Chang's breach goes back to September 2013, predating the breach that impacted big-box retailer Target Corp. in November and coming on the heels of the breach that compromised Neiman Marcus in July. An executive at another card issuer says the new timeline for the breach suggests a stronger connection to previous retail compromises, which could be a good thing for issuers that have already replaced cards impacted by the breaches at Target, Sally Beauty and Michaels.

http://www.govinfosecurity.com/pf-changs-breach-predates-target-a-6968?rf=2014-06-20-eg&utm_source=SilverpopMailing&utm_medium=email&utm_campaign=enews-gis-20140620%20(1)&utm_content=&spMailingID=6680650&spUserID=NTQ5MzMzMDA3ODES1&spJobID=462174230&spReportId=NDYyMTc0MjMwS0

Code hosting Code Spaces destroyed by extortion hack attack

This is an instance of a small business being ruined by a cyber attack. While most of us don’t run a completely cyber business, how would your business do if you had most of your network/computers data deleted or encrypted and held for ransom?

Cloud code hosting service Code Spaces is forced to shut down, as a DDoS attack coupled with an unsuccessful extortion attempt was followed by the attacker deleting most of its code repositories and backups. According to the notice on the service's website, the DDoS attack started on Tuesday. The company then noticed that a number of messages were left by the attacker on their Amazon EC2 control panel, meaning that he or she had access to it.

The identity of the attacker is still unknown, as well as how he or she was able to access the control panel. The service says that they have "no reason to think its anyone who is or was employed with Code Spaces.“ The initial internal investigation revealed that no machine access had been achieved by the attacker. Not wanting to pay the large fee requested by the attacker to stop the DDoS attack, they attempted to regain control of the panel by changing passwords.

Unfortunately for them, the intruder was prepared for that attempt, and had already created a number of backup logins. He retaliated by proceeding to randomly delete artifacts from the panel. "We finally managed to get our panel access back but not before he had removed all EBS snapshots, S3 buckets, all AMI's, some EBS instances and several machine instances," they shared. "In summary, most of our data, backups, machine configurations and offsite backups were either partially or completely deleted."

"Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in a irreversible position both financially and in terms of on going credibility," they explained. "As such at this point in time we have no alternative but to cease trading and concentrate on supporting our affected customers in exporting any remaining data they have left with us."

"All that we can say at this point is how sorry we are to both our customers and to the people who make a living at Code Spaces for the chain of events that lead us here," they concluded. "We hope that one day we will be able to and reinstate the service and credibility that Code Spaces once had!"

Users across the web are commenting on the fact that the company promised regular, off-site backups, but failed to mention that those backups were accessible via the AWS control panel. Also, it seems obvious that they haven't used multi-factor authentication to secure the AWS account, even though the option is there.

http://www.net-security.org/secworld.php?id=17028