CYBER SECURITY

Newsletter

October 2013

Aim of the long-term CENAA program on cyber security (Global Netizenship in Cyberworld - GNC) is in-depth analysis of multi-spectral and cross-cutting issues of national and international security. In last years, cyber attacks have become powerful and fully-fledged tool in conventional war and industrial espionage. Through establishing network of national and international partnerships, CENAA strives to ensure that cyber security will get into focal point of political, corporate and expert elites. Goal of this Newsletter and GNC project is also de-tabuise issue of cyber security to all.

October 1, 2013

CYBERSECURITY IS EVERYONE'S BUSINESS

I wish it were possible to simply delegate cybersecurity to the "big guys." Why not just let the government and big companies handle it? Forbes, October 1, 2013

http://www.forbes.com/sites/larrymagid/2013/10/01/cybersecurity-is-everyones-business/

October 2, 2013

WHY MERE COMPLIANCE INCREASES RISK

In some cases, poor training is as bad as–if not worse than–no training it all, say John Schroeter and Tom Pendergast.

The Department of Health and Human Services recently confirmed that a lack of training is a common cause of HIPAA compliance difficulties. But is that really such a surprise? Given the poor state of awareness training in many organizations, it's no wonder that HIPAA violations are actually on the rise. The fact is, to achieve formal, "letter of the law" compliance, just about any form of training will do to "check the box." But as we continue to see, bad training is, in the final analysis, practically

equivalent to–or worse than–no training at all, and hence the disappointing results reported by HHS and by others who wonder why their compliance training fails. CSO, October 2, 2013

http://www.csoonline.com/article/740820/why-mere-compliance-increases-risk?source=rss_security_leadership

October 4, 2013

THE PRACTICALITY OF THE CYBER KILL CHAIN APPROACH TO SECURITY

Lysa Myers of the InfoSec Institute explains the Cyber Kill Chain approach and whether or not it's a good fit for certain organizations.

If you're one of those folks who read a lot of InfoSec news, you've no doubt heard a lot of mention of the effectiveness of a Cyber Kill Chain approach to security. If you managed to miss the hubbub, you may be wondering if that's the latest sci-fi movie starring the usual muscle-bound action hero. In this article we'll talk about what a Cyber Kill Chain approach is, and whether it might be a good fit for your organization. CSO, October 4, 2013

http://www.csoonline.com/article/740970/the-practicality-of-the-cyber-kill-chain-approach-to-security?source=rss_security_leadership

October 8, 2013

ADOBE, MICROSOFT PUSH CRITICAL SECURITY FIXES

Adobe and Microsoft today each issued software updates to fix critical security issues in their products. Microsoft released eight patch bundles to address 26 different vulnerabilities in Windows and other software – including not just one but two zero-day bugs in Internet Explorer. KrebsOnSecurity, October 8, 2013

http://krebsonsecurity.com/2013/10/adobe-microsoft-push-critical-security-fixes-3/

October 9, 2013

SUSPECT IN 'BLACKHOLE' CYBERCRIME CASE ARRESTED IN RUSSIA: SOURCE

(Reuters) - Russian authorities have arrested a man believed to be responsible for distributing a notorious software kit known as "Blackhole" that is widely used by cyber criminals to infect PCs, according to a person familiar with the situation. Reuters, October 9, 2013

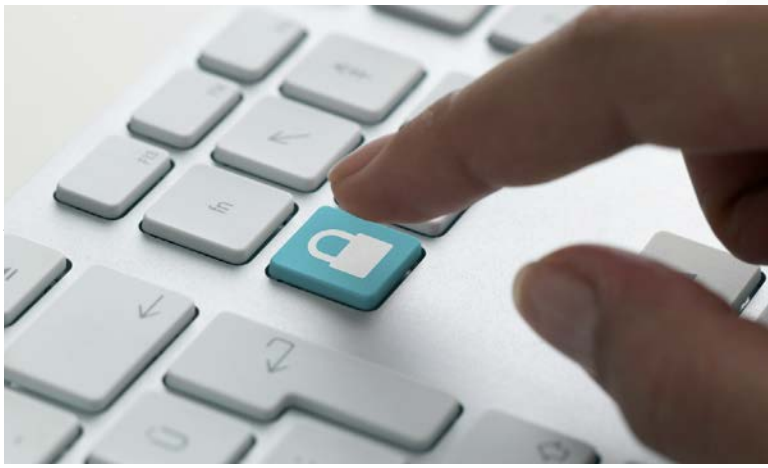
http://www.reuters.com/article/2013/10/08/cybercrime-arrest-idUSL1N0HY26I20131008

October 10, 2013

NORDSTROM FINDS CASH REGISTER SKIMMERS

Scam artists who deploy credit and debit card skimmers most often target ATMs, yet thieves can also use inexpensive, store-bought skimming devices to compromise modern-day cash registers. Just this past weekend, for instance, department store chain Nordstrom said it found a half-dozen of these skimmers affixed to registers at a store in Florida. KrebsOnSecurity, October 10, 2013

http://krebsonsecurity.com/2013/10/nordstrom-finds-cash-register-skimmers/



October 13, 2013

PRIVACY FEARS GROW AS CITIES INCREASE SURVEILLANCE

OAKLAND, Calif. — Federal grants of $7 million awarded to this city were meant largely to help thwart terror attacks at its bustling port. But instead, the money is going to a police initiative that will collect and analyze reams of surveillance data from around town — from gunshot-detection sensors in the barrios of East Oakland to license plate readers mounted on police cars patrolling the city's upscale hills. The New York Times, October 13, 2013

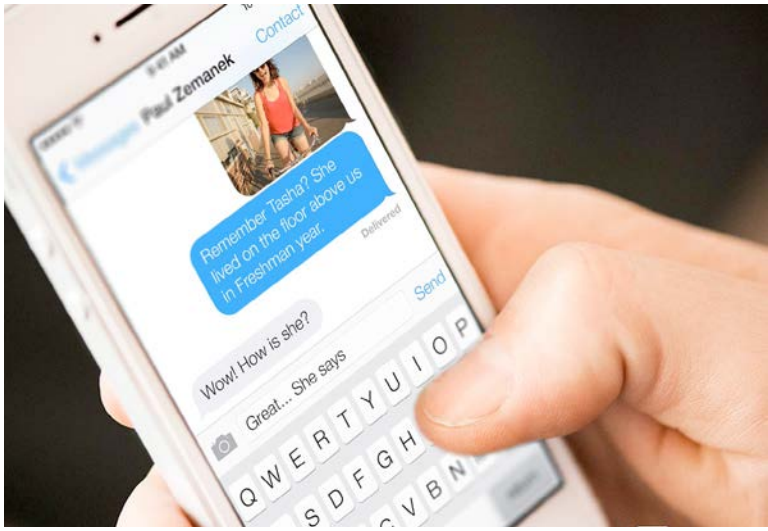
http://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html?hp&_r=1&

October 14, 2013

THOUSANDS OF SITES HACKED VIA VBULLETIN HOLE

Attackers appear to have compromised tens of thousands of Web sites using a security weakness in sites powered by the forum software vBulletin, security experts warn. KrebsOnSecurity, October 14, 2013

http://krebsonsecurity.com/2013/10/thousands-of-sites-hacked-via-vbulletin-hole/



October 18, 2013

APPLE IMESSAGE OPEN TO MAN IN THE MIDDLE, SPOOFING ATTACKS

The Apple iMessage protocol has been shrouded in secrecy for years now, but a pair of security researchers have reverse-engineered the protocol and found that Apple controls the encryption key infrastructure for the system and therefore has the ability to read users' text messages–or decrypt them and hand them over at the order of a government agency. ThreatPost, October 18, 2013

http://threatpost.com/apple-imessage-open-to-man-in-the-middle-spoofing-attacks/102610

October 18, 2013

VERIFY, THEN TRUST

ONE of the many outcomes of Edward Snowden's leaks was to confirm what security researchers had long nervously joked about—that Western intelligence agencies spend a great deal of time and money trying to undermine the cryptographic software that secures computers all over the world (similar suspicions swirl around the Chinese and Russian spy agencies, too). The documents suggest that the spies lean on firms to build "back doors" into their products, infiltrate those companies with their own employees, and work to nobble cryptographic standards. The Economist, October 18, 2013

http://www.economist.com/blogs/babbage/2013/10/computer-security

CYBER RISK AND THE BOARD OF DIRECTORS—CLOSING THE GAP

The responsibility of corporate directors to address cyber security is commanding more attention and is obviously a significant issue. Yet here is how one writer entitled her Forbes article about the 2012 Carnegie Mellon Cylab Report: "Boards Are Still Clueless About Cybersecurity."

Corporate boards have a duty to protect corporate assets, whatever the form these assets take. Increasingly, corporate assets consist of information. In some companies, digital information constitutes most of the assets of the enterprise. Even in industries not commonly thought of as "hi-tech"–such as energy and utility companies–computers and software play a major role in finance, management and operations and the most sensitive and mission-critical functions are, with few exceptions, computerized. Bloomberg Law

http://about.bloomberglaw.com/practitioner-contributions/cyber-risk-and-the-board-of-directors-closing-the-gap/

October 22, 2013

NATO DEFENCE MINISTERS MOVE FORWARD WITH CONNECTED FORCES AGENDA

On 22nd October 2013, defence ministers of the NATO member states, on their regular meeting, discussed cyber-defence issues. They stated that the Alliance should cooperate to upgrade its capabilities to protect the networks of the member states and networks of Alliance itself. As general secretary concluded: "Cyber defence is a national responsibility. But we all agree that NATO can, and should, play a useful role to facilitate the development of strong national cyber defence capabilities".

http://www.nato.int/cps/en/natolive/news_104241.htm

October 23, 2013

LANDMARK LEADERSHIP CONFERENCES FOR IT EXECUTIVES:

The IT Summit is the executive technology conference series returning to Los Angeles for our seventh annual event on October 23, 2013. The purpose of the summit is to provide educational and networking resources for the IT leaders in Southern California. The conference is

driven by an Executive Board of regional IT professionals that directs the content of the conference. The IT Summit is designed to address the real-world opportunities and challenges faced by today's executives. The IT Summit, Event Date: October 23, 2013

http://www.theitsummit.com/event/los-angeles-2013/

October 25, 2013

AMID NEW STORM IN U.S.-EUROPE RELATIONSHIP, A CALL FOR TALKS ON SPYING

BERLIN — While President Obama has tried to soften the blow, this week's disclosures about the extent of America's spying on its European allies have added to a series of issues that have sharply eroded confidence in the United States' leadership at a particularly difficult moment. The New York Times, October 25, 2013

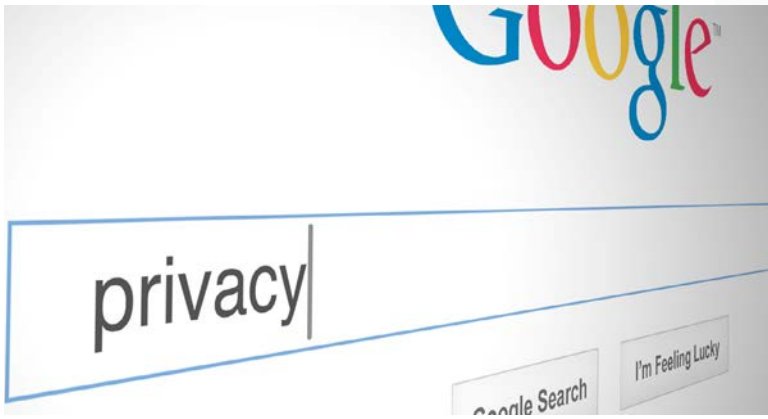
http://www.nytimes.com/2013/10/26/world/europe/fallout-over-american-spying-revelations.html

October 30, 2013

THE 28TH ANNUAL 2013 ISSA SOCAL SECURITY SYMPOSIUM

The SoCal Security Symposium features over 30 vendor exhibits and several industry experts discussing current security issues such as eDiscovery, cloud security, threat vectors, mobile security, and much more. There will be lots of give a ways and prizes! This conference will provide tremendous networking opportunities. You'll come away with advice and knowledge you can start applying to your environment immediately. Your registration will include your breakfast, lunch, ice cream social, CPE credits (8) and entrance into the conference sessions and exhibit area. ISSA of Orange County, Event Date: October 30, 2013

http://www.issa-oc.org/conference.html



October 31, 2013

NSA ACCUSED OF HACKING GOOGLE, YAHOO DATA LINKS

The US National Security Agency has reportedly broken into links that connect Yahoo and Google data centers around the world. The latest revelations came hours after German and US officials met to discuss US spy claims. The Washington Post newspaper published documents on Wednesday which suggest that the US National Security Agency (NSA) secretly broke into key main communication links from Yahoo and Google data centers around the world. DW, October 31, 2013

http://www.dw.de/nsa-accused-of-hacking-google-yahoo-data-links/a-17195593

COMING UP IN NOVEMBER

Slovak Strategic Forum (SSF) is exclusive platform for discussion about actual international and national security issues by experts from the government, private sphere and academia. SSF is organized regularly twice a year, in the spring and autumn. Since 2007 ten forums have been organized with goal to map the positions of Slovak security experts and provide the recommendations for decision makers. The topic of the next SSF will be cyber-security.

CENAA

Tolstého 9
811 06 Bratislava
E-mail: office@cenaa.org