Szarvák Anikó

Something's missing from a safe cyber world

This article highlights a serious flaw in security awareness. Through some examples the article presents the key problems and shows a different method to solve the root cause.

People – users, administrators, managers – need to be educated according to the new cyber challenges and they need to understand the significance of the this whole new and complex IT world.

In my understanding we have just stepped into a new era in the field of info-communication and we – all of us – must start handling the recently developed risks in a proper way to ensure privacy and security.

Keywords: safe internet, security awareness, education

Introduction

Let me start this article with a short conversation with a 30-year-old contractor.

I asked him about his smartphone, why does he use it without a PIN? His answer was simple:

'Why should I use one? There's nothing interesting on my phone!' His reaction showed no fear. While he does not secure his smartphone he locks all the doors and windows of his office and home and uses an alarm system for his car…

For years, the number of personal computers has been growing, mobile phones are now smartphones and their usage has exploded. I assume that this is just the beginning. We are using information technology for almost anything, and the IoT – the Internet of Things – is just one step ahead. While I watch this spread of computers I wonder: will education catch up and start a new line of didacticism on teaching how to use the internet instead how to use some software.

When the "Internet" showed up, new threats popped up as well

What should we know about the growth of the Internet? CISCO has made a Global Mobile Data Traffic Forecast by Region in early 2015.

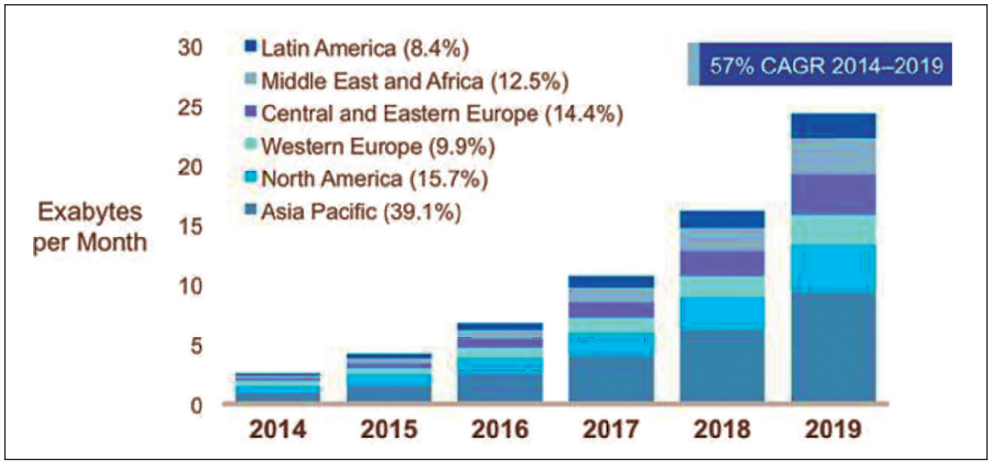


Figure 1. CISCO Global Mobile Data Traffic Forecast by Region

Source: www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html

The speed of the growth of mobile Internet traffic is exponential. This means that end users of the Internet are really connected and they have fast growing mobile penetration. This means also those users - aka customers - use the internet to make their days easier, buying food and assets online, managing their needs online, talking, chatting and doing their ordinary things online.

From a cyber security perspective, users give more "attack surface" without knowing about it. This express growth of Internet traffic also means that companies - including financial, healthcare, tech, energy, etc. - and even the government reaches their customers via the Internet. They provide services through the World Wide Web.

Let me draw a parallel between using the Internet – including usage of free services – and driving a car. Before I got my driving license I had to pass a paper based test about driving rules, had to take a successful routine exam and finally drove a car in traffic flawlessly. Is driving – or any other vehicle driving – a dangerous thing? My opinion is a hundred percent yes.

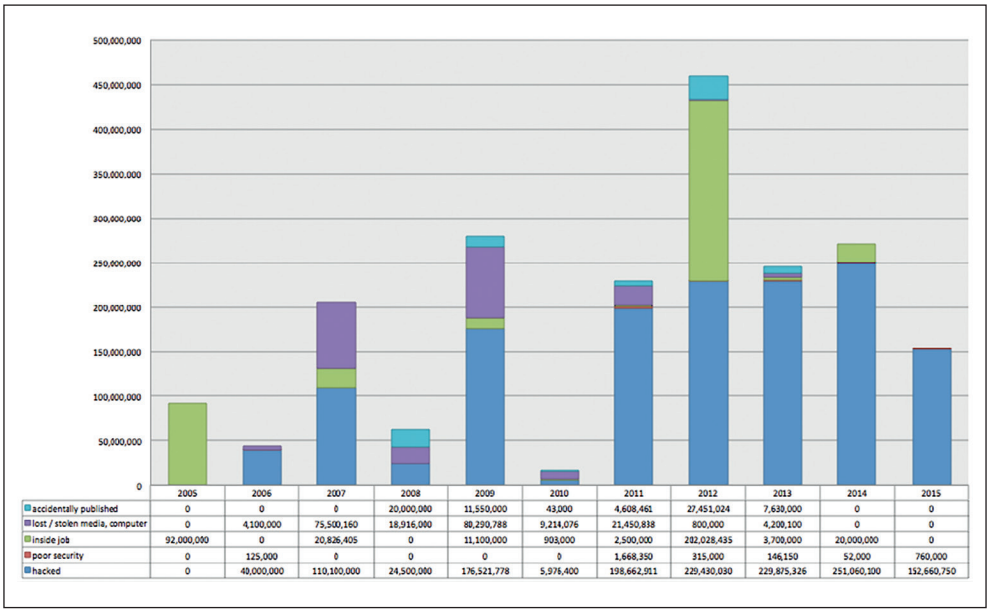
Using the Internet is license-free. You just have to have an Internet capable mobile with a data plan on it or just catch "free WiFi" and you just simply access it. Is there a possibility to steal all your credentials, your bank account information or all of your stored

data from the device even your identity? Is it dangerous? You can connect without any knowledge on privacy and your rights? Unfortunately most of the Internet users are in danger because of lack of knowledge.

A very simple example: lots of the users give and store their bank account information while they are buy things at a web shop. They do not care if the web shop stores they sensitive data for "easier further shopping"; this means if somebody has accesses to the database unwarrantedly, they can use that bank account for buying things on the Internet as well.

I will admit that this example is a bit harsh. Let me give you another one: A simple user on a community site posts that he just won the lottery. He bought a lot of new stuff: jewels, new plasma TV, cool games for kids. He posts pictures about it then packs the family and travels around the world. Of course this information could be shared with anybody. Is it a surprise when they come back from the holiday and all the new things are gone? They asked to be robbed!

For these reasons I suggest educating Internet users and users working for companies and taking care of the companies' data, as well as their own data.



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
accidentally published	0	0	0	20,000,000	11,550,000	43,000	4,608,461	27,451,024	7,630,000	0	0
lost / stolen media, computer	0	4,100,000	75,500,160	18,916,000	80,290,788	9,214,076	21,450,838	800,000	4,200,100	0	0
inside job	92,000,000	0	20,826,405	0	11,100,000	903,000	2,500,000	282,028,435	3,709,000	20,000,000	0
poor security	0	125,000	0	0	0	0	1,668,350	315,000	146,150	52,000	760,000
hacked	0	40,000,000	110,100,000	24,500,000	176,521,778	5,976,400	198,662,911	229,430,030	229,875,326	251,060,100	152,660,750

Figure 2: World's Biggest Data Breaches

Source: www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

From this chart it is obvious that data mostly is stolen via hacker attacks, possibly targeted attacks. The companies, which are affected by these attacks are well regulated by government. They take the necessary and sufficient steps to secure their customer data. However, a successful cyber attack is just matter of time.

Let me introduce some necessary and sufficient steps. There must be the controls. Just a few sentences to be clear what we have to do in security, especially from a cyber security perspective:

We have technical and administrative controls. Administrative controls could be written, and verbal or behavioral routines. Unfortunately they are mostly "read once then put on the shelf". Technical controls are placed with additional security systems or settings on information systems themselves.

From a different viewpoint, both administrative and technical controls could be preventive, detective and corrective ones. Most of the time, the focus is on preventive controls instead of detective and corrective ones.

Most of the cyber attacks find weaknesses. Basically in a web service there is a good chance to find a vulnerability that can lead to a successful attack. I usually browse the OWASP website about new techniques and countermeasures.

The Open Web Application Security Project (OWASP) is a worldwide non-profit charitable organization focused on improving the security of software. OWASP's mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

They prepare TOP 10 statistics on a 3 years basis about the most used techniques and vulnerability types. In the next table there is a summary about it.

The following techniques are common during each period:

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser, which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys or session tokens or to exploit other implementation flaws to assume other users' identities.

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests for the vulnerable application, thinking those are legitimate requests from the victim.

A direct object reference occurs when a developer exposes a reference to an internal implementation object such as a file, directory, or database key. Without an access control check or other protection attackers can manipulate these references to access unauthorized data.

TOP	2007	2010	2013
1	Cross Site Scripting (XSS)	Injection	Injection
2	Injection	Cross Site Scripting (XSS)	Broken Authentication and Session Management
3	Malicious File Execution	Broken Authentication and Session Management	Cross Site Scripting (XSS)
4	Insecure Direct Object Reference	Insecure Direct Object References	Insecure Direct Object References
5	Cross Site Request Forgery (CSRF)	Cross Site Request Forgery (CSRF)	Security misconfiguration
6	Information Leakage and Improper Error Handling	Security misconfiguration	Sensitive Data Exposure
7	Broken Authentication and Session Management	Insecure Cryptographic Storage	Missing Function Level Access Control
8	Insecure Cryptographic Storage	Failure to Restrict URL Access	Cross Site Request Forgery (CSRF)
9	Insecure Communication	Insufficient Transport Layer Protection	Using Components with Known Vulnerabilities
10	Failure to Restrict URL Access	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards

Figure 3, OWASP top 10 by years 2007, 2010 and 2013

Source: www.owasp.org

All of these types of attacks have a prevention guide with documentation, how-to databases all over the Internet. These attacks could be avoided with proper configuration. For more technical countermeasures I suggest seeing the SANS related poster called "20 critical security control".

If you just think: 'It is really that easy, these attacks should be eliminated by now!' I assume that you could be right. So what is the root cause that these types of attacks still exist? My opinion is based on the "human". To understand it, let us make the definition of Information System clear: a computer Information System (IS) is a system composed of people and computers that processes or interprets information.

If we have enough information and technical resources to secure computers and networks then the only weakness that remains is people.

If we are talking about a company we can define three kind of human resources according to responsibilities:

– Users,
– Administrators,
– Managers.

I already wrote about user-behavior. Let me write about Administrators. They are the heart and the soul of information systems. They are able to build up the systems and connect the information through networks and let information be visible to users.

In most cases the ultimate reason why administrators are essential to run an online information system is business continuity. But does business continuity mean only that the system is up and running? From the management perspective the short answer could be yes, without hesitation. But the responsible answer should be something like this: 'administrators are essential to run online information systems securely'.

And here comes the next question, how can you ensure that your system is up and running and desirably secure? To complicate the question let me put the "cost effectively" phrase into it.

There is a saying: "Cheap, fast, good – you can choose two of the three". Turn this into an information system security phrase: 'Usable, operable, secure…'. In most cases usable and operable are the chosen ones. After a cyber attack those choices will change but the question remains: 'How will the administrator secure the information system? There are hundreds and thousands of hardening documentation available. There are lots of company policies, regulations and recommendations on information system security. Is it still necessary to wait for a cyber attack?

I can imagine a new state of secure information system operation. But to reach this new state education is needed. The management needs to be given time and resources to administrators to learn: cyber security is essential and not a supplementary thing.

Look for a special administrator type: developer. From a management perspective, development must be fast and cheap. From an operation perspective, development should be fast and good. From a cyber threat point of view at the end of the day all basic cyber security countermeasures are up to the developer who has to 'choose two of the three' possibilities.

In addition, I desire a well-targeted education program for developers that can achieve web based vulnerabilities' elimination. Do not think that I believe all security flaws are fixable. I believe that if the development acceptance criteria could be changed from "functionality defined" to "only defined functionality" the numbers and depth of security flaws will drop dramatically.

Based on ISMS (Information Security Management System) recommendation "management" has to ensure the resources for proportional risk mitigation. As a matter of fact the management is responsible for the information. In risk management – based on my experience – cyber threat, cyber attacks are underestimated. The choice is up to you to decide in this case whether the risk management processes are defective or the management decisions are inappropriate which mostly depends on risk management.

To see this question in a different way: If you have a car and somebody crashes into its back, it is visibly damaged. When we talk about cyber crime then a hacker or an industrial spy stole data through the companies' website but the website is still running: it is not visible damage at that time.

The damage will be visible and convertible into money such as a situation when the stolen data is bank account information and the thief starts to buy things with it. The company's customer will prosecute the company because of illegal usage of his or her bank account.

To avoid these incidents management should be educated and have to understand that detective controls are as essential as preventive controls. These days I would suggest as reliable this threat overview from the Hackmageddon statistics:

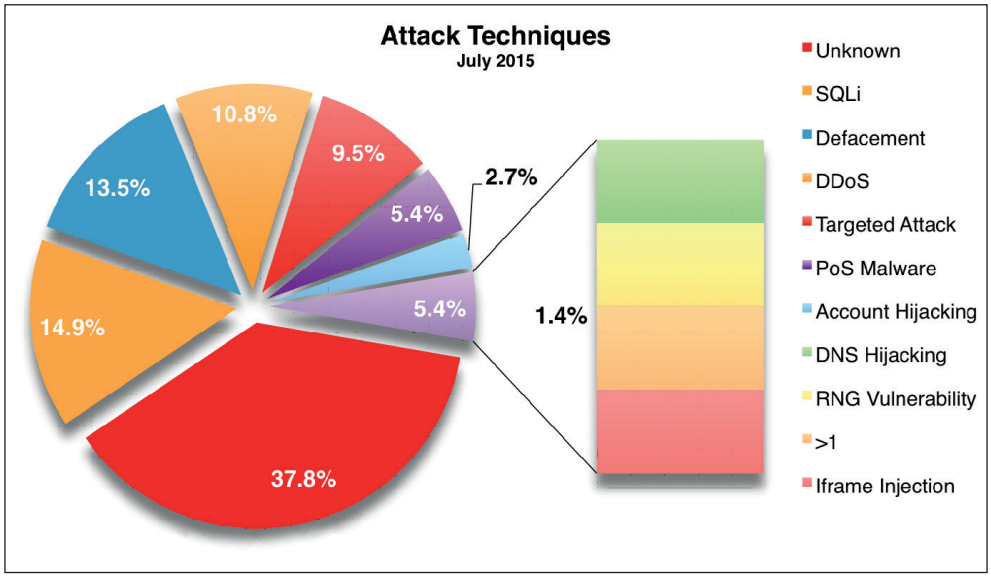


Figure 4. Hackmageddon attack techniques diagram in:

Source: www.hackmageddon.com/2015/08/10/july-2015-cyber-attacks-statistics/

These attacks are happening now and happening on the World Wide Web. Which means geo-location, the physical border of states does not matter.

For me it is obvious that people – I mean users, administrators and managers – should be educated. In this case the awareness is not enough in school or their education program of informatics.

These days we are in the middle of a war, fighting this battle with zeros and ones. The companies should not have to send their employees into war with knives if the opposite side uses guns.

Well-trained, careful and aware users in the information security field are not a privi-

lege, they should be a must in companies, all over the world, in every place. The education program in schools should change from focusing on software skills, learning what to use into "how" to use it and make real knowledge on the importance of their behavior.

Now let me show you something about the big picture!

Cyber Crime is any crime that involves a computer and a network; a criminal activity where a computer may have been used in commission of a crime or it may be a target. Dr. Debarati Halder and Dr. K. Jaishankar (2011) define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"

Hacktivism or hactivism (a portmanteau of hack and activism) is the subversive use of computers and computer networks to promote a political agenda. With roots in hacker culture and hacker ethics, its ends are often related to the free speech, human rights, or freedom of information.

Cyber espionage is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers.

Cyber warfare has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".

Let us travel back in time to 2012. What was the motivation behind the attacks?

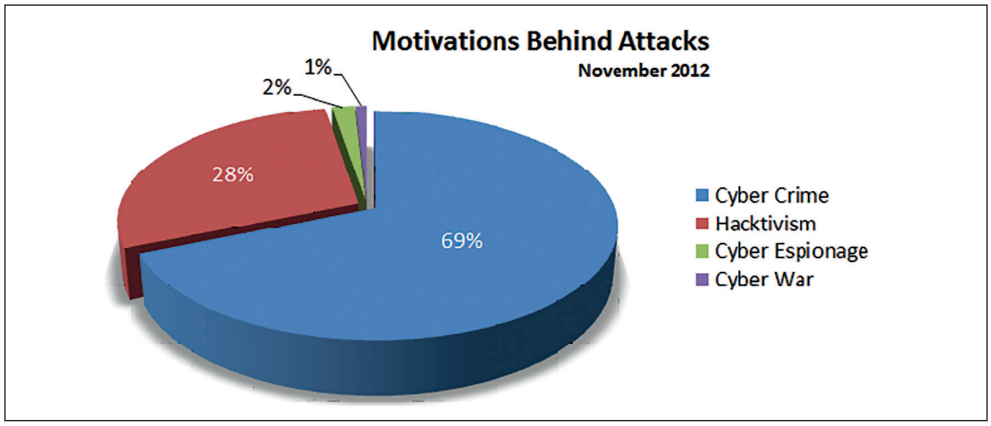


Figure 5, Hackmageddon statistics, Motivation behind Attacks, November 2012

Source: www.hackmageddon.com/2012/12/09/november-2012-cyber-attacks-statistics/

There is another diagram about motivation behind attacks. It is from the present:

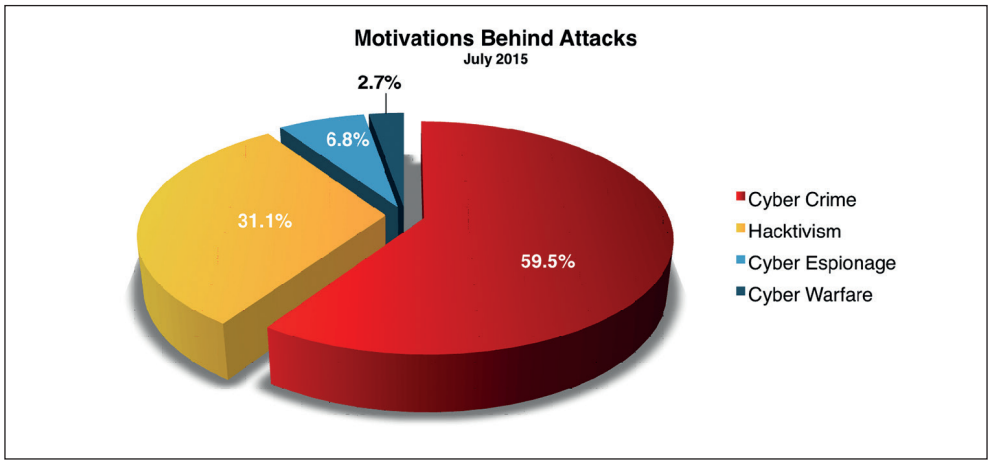


Figure 6, Hackmageddon statistics, Motivation behind Attacks, July 2015

Source: www.hackmageddon.com/2015/08/10/july-2015-cyber-attacks-statistics/

From the Hackmageddon statistics it is obvious that there are no new motivations behind cyber attacks, but on the other hand just read these diagrams in a correct way: cyber espionage has been growing but all the other type of motivations – Hactivism and Cyber Crime – has nearly the same percentage. For me these diagrams show that - assuming that Cyber Espionage is a paid activity - there is a brand new line of business that has been growing these past years.

References:

CISCO Global Mobile Data Traffic Forecast by Region, in: www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html

Clarke, Richard A.: *Cyber War.* HarperCollins (2010) ISBN 9780061962233

Computer crime in: https://en.wikipedia.org/wiki/Computer_crime

Cyber espionage in: https://en.wikipedia.org/wiki/Cyber_spying

Cyber warfare in: https://en.wikipedia.org/wiki/Cyberwarfare

D'Atri A., De Marco M., Casalino N. (2008): *Interdisciplinary Aspects of Information Systems Studies.* Physica-Verlag, Springer, Germany, pp. 1-416, doi 10.1007/978-3-7908-2010-2 ISBN 978-3-7908-2009-6

Hackmageddon attack techniques diagram and motivation behind attacks, July 2015 in: www.hackmageddon.com/2015/08/10/july-2015-cyber-attacks-statistics/

Hackmageddon motivation behind attacks, November 2012 in: www.hackmageddon.com/2012/12/09/november-2012-cyber-attacks-statistics/

Hactivism in: https://en.wikipedia.org/wiki/Hacktivism

Krapp, Peter (Fall 2005): "Terror and Play, or What was Hacktivism? " Grey Room". MIT Press. Retrieved 2013-02-28.

Moore, R. (2005): *Cyber crime: Investigating High-Technology Computer Crime.* Cleveland, Mississippi: Anderson Publishing.

Open Web Application Security Project Top Ten Vulnerability in: www.owasp.org/index.php/Main_Page

SANS Resources, 20 critical security controls in: www.sans.org/security-resources/posters/20-critical-security-controls-55/download

Warren G. Kruse, Jay G. Heiser (2002): *Computer forensics: incident response essentials.* Addison-Wesley. p. 392. ISBN 0-201-70719-5.

World's biggest data breaches, in: www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Egy hiányzó dolog a biztonságos kibervilághoz

Szarvák Anikó

Jelen cikk célja rávilágítani egy kritikus biztonsági hiányosságra. Példákon keresztül bemutatja a kulcsproblémát, és egy, a szokásostól eltérő megoldást mutat a probléma megoldására.

Az embereknek – felhasználóknak, üzemeltetőknek, vezetőknek – szükségük van oktatásra az új kibervilág kihívásairól, és meg kell érteniük ennek a teljesen új és komplex IT-világnak a jelentőségét.

Meglátásom szerint csak most léptünk egy új érába az infokommunikáció területén, és mindannyiunknak el kell kezdenünk kezelni az újfajta kockázatokat biztonságunk érdekében.

Kulcsszavak: biztonságos internet, biztonságtudatosság, oktatás