GLOBAL CYBER SECURITY CENTER

Newsletter

2018 January

Cyber Security is our mission

editorial

When sport can become a national security issue.

It seems that history repeats itself and you never learn the lesson. It was the year 2010 when Foursquare service invited its users to do the “check-in” in popular places and then transmit all these data publicly by mistake.
Are not you convinced yet? Try to open Google Maps and select from the menu "Timeline"; unless you have disabled Google access to your location data, you will see a clear map of your movements punctually referable also temporally enabling the calendar view.
We must think that the data represent the entire business model for these companies and it is therefore difficult for them to find a reason to stop the collection.
You may wonder why we are still talking about this topic, why the umpteenth article on data sharing? Because in these days all the newspaper where talking about Strava. This is an application for monitoring athletic activity, Strava is able to manage and elaborate with great details the data of runners and cyclists. Everything starts, as always, from our smartphone, the Strava App is free and is available for iOS and Android, the application allows us to record the GPS track of our race or ride. The app tells us what were our times, the paths, the miles and we can make transform this solitary training in a viral challenge. Some numbers? In December 2016, Strava announced that more than 300 million sports activities were loaded; of these activities 26.90% have been carried out in group collecting more than 1.3 billion Kudos (Kudos are the correspondents to the likes of Facebook). What happened? Strava in November 2016 published the maps that collected all the sports activities, which, again to give you some numbers, referred to a total of 27 billion kilometers. The issue was that some of the App users work for militaries or intelligence agencies. At that point some security experts were able to connect the dots and create a relation between bases or locations of US military / intelligence operations.
All was accelerated by Nathan Ruser, a student studying international security at the Australian National University; he started to post Twitter a series of images that pointed out Strava user activities potentially related to US military bases in Afghanistan, Turkish military patrols in Syria, and much more. The Department of Defense is going to revise the IoT and wearable devices and is also said it encourages all defense personnel to limit their public presence on the Internet and of course the guidance is even stricter when troops operate in sensitive locations. As we have written several times the awareness in the use of these tools plays a fundamental part and we need to work a lot more on the awareness to create a generation of users aware in the digital world. Many areas of improvement in this area that must see manufacturer, service companies and consumer associations work together. And last but not least, programs in schools that educate on cybersecurity.

Enjoy your reading

Nicola Sotira
General Manager GCSEC

events

RECON Brussels 2018
Location: Brussels, Belgium
Date: February 2-4, 2018
https://recon.cx/2018/brussels/
RECON is a computer security conference held annually in Brussels (Belgium) and Montreal (Canada). Recon is the world’s largest global gathering of retail real estate professionals. Join leading developers, owners, brokers and retailers to conduct a year’s worth of business under one roof, in record timeoffers a single track of presentations over the span of three days with a focus on reverse engineering and advanced exploitation techniques.

Italian Conference on Cybersecurity (ITASEC18)
Location: Milan, Italy
Date: February 6-9, 2018
https://www.itasec.it/
The Second Italian Conference on Cyber Security (ITASEC18) is an annual event supported by the CINI Cybersecurity National Laboratory that aims at putting together Italian researchers and professionals from academia, industry, and government working in the field of cyber security. The conference will be structured into a main cyber security science and technology (S&T main track), included a sequence of multidisciplinary sessions from economic sciences, political sciences, laws etc on a specific hot topic in cyber security, and a demo track devoted to prototypes developed by industries, research centers and universities.

Cyber Security Summits 2018
Location: San Jose, California, USA
Date: February 13, 2018
https://cybersummitusa.com/siliconvalley18/
The Cyber Security Summit is an exclusive conference series connecting C-Level & Senior Executives responsible for protecting their companies’ critical infrastructures with cutting-edge technology providers & renowned information security

in this number

7 Awesome Skills That Will Make You Stand Out As A CyberSecurity Pro

by Marco Essomba – Founder and Executive Chairman, iCyber-Security

Originally published at www.linkedin.com

Are you an IT Graduate or Network Security Engineer looking to enhance your career and stand out from the crowd? This article is for you.

I have been in the network & security space for more than a decade. As a network security engineer, security consultant, and now Founder & CTO at iCyber-Security Group, these products have served me well over the years in order to rise above the crowd. Note that the list below is not sponsored or endorsed by those vendors. It is drawn from my own past experience and it is by no means the absolute truth. I am biased to the extent that I have grown to love the products, I list below over the years.

1. Routing & Switching Technologies

- **What: Cisco** is the de-facto vendor for routing and switching with a big chunk of the enterprise market.
- **Why:** Given the ubiquitous presence of Cisco routers and switches in the enterprise space it is worth spending the time to learn Cisco R&S well and gain a theoretical and practical knowledge of the product.
- **Where to start**: Download a simulator like GNS3 or VIRL http://virl.cisco.com/ or Eve-NG: http://eve-ng.net

2. Firewall Technologies

- **What: Check Point Technologies** is one of the most popular enterprise perimeter firewalls.
- **Why:** The Check Point Firewall adoption remains high with Fortune 500 customers due to its simple and intuitive user interface as well as its powerful inspection engine. Certification and hands on expertise is very desirable.
- **Where to start:** Start with Check Point R80 Firewall. It is available to download as a virtual appliance.

3. Intrusion Detection & Prevention Systems

- **What: Sourcefire** is now part Cisco. Based on the Snort engine Sourcefire is the IPS/IDS of choice for many enterprise customers. With the recent Cisco acquisition it will continue to grow within the enterprise space.
- **Why:** Sourcefire and Snort will teach you lots of tricks when it comes to intrusion detection and prevention going from simple cyber attacks protection to the most sophisticated defence tactics.
- **Where to start:** Download a free version of Snort from https://snort.org/downloads. Sourcefire trial is available at https://www.cisco.com/c/en/us/services/acquisitions/sourcefire.html.

experts and has been ranked as one of the "Top 50 Must-Attend Conferences" for the last two years by DigitalGuardian.

Network and Distributed System Security Symposium (NDSS)
Location: San Diego, California, USA
Date: February 18–21, 2018
https://www.ndss-symposium.org/ndss2018/
NDSS fosters information exchange among researchers and practitioners of network and distributed system security. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of available network and distributed systems security technology.

CyberThreat 2018
Location: London, UK
Date: February 27-28, 2018
https://cyberthreat2018.com/
CyberThreat 2018 is a new event designed to bring together the UK and Europe's technical cyber security community. Focused on practitioners and spanning the full breadth of cyber defence and incident response disciplines, the event encourages sharing of bleeding edge techniques, case studies from the field and new tools.

news

Meltdown and Spectre attacks affect almost any processor, including Intel, ARM, AMD ones
http://securityaffairs.co/wordpress/67394/hacking/meltdown-spectre-attacks.html
The Meltdown and Spectre attacks could allow attackers to steal sensitive data which is currently processed on the computer.
Almost every modern processor is vulnerable to the 'memory leaking' flaws, this has emerged from technical analysis triggered after the announcement of vulnerabilities in Intel Chips.
White hackers from Google Project Zero have disclosed the vulnerabilities that potentially impact all major CPUs, including the ones manufactured by AMD, ARM, and Intel. The expert devised two attacks dubbed Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753 and CVE-2017-5715), which could be conducted to sensitive data processed by the CPU.
Both attacks leverage the "speculative execution" technique used by most modern CPUs to optimize performance.

What is FakeBank? New banking malware can intercept SMS messages to steal sensitive data and funds
http://www.ibtimes.co.uk/what-fakebank-new-banking-malware-can-intercept-sms-

4. Secure Web Gateways

- **What: Clearswift** is renowned for its MIMEsweeper Content Inspection Engine that protects email and web transactions against malware.
- **Why:** As cyber security continues to be a major challenge for small and large organisations, protecting enterprise data at rest and in motion is hot topic.
- **Where to start:** Start with the Clearswift SECURE Web Gateway. Request a demo and trial from https://www.clearswift.com/contact-us#demo.

5. Application Delivery Controllers (ADC)

- **What: F5 Networks** leads the Application Delivery Controllers (ADC) market. F5 most popular product is F5 LTM which helps enterprises to deliver “Applications Without Constraints”.
- **Why:** ADCs are crucial for the delivery of Enterprise Apps in a fast, secure, and resilient manner. Since mobile apps now rule the world F5 ADCs demand will continue to grow**.**
- **Where to start:** Start with the F5 LTM. Request a trial download from https://f5.com/products/trials/product-trials.

6. Two-Factor Authentication

- **What: RSA** is one of the leaders in enterprise two-factor authentication solutions.
- **Why:** The increasing number of cyber attacks means security remains a hot topic. Strong authentication is still one of the most effective first line of defence against cyber criminals.
- **Where to start:** Start with RSA SecurID. You can request a trial from https://www.rsa.com/en-us/products/rsa-securid-suite or contact me.

7. Operating Systems and APIs

- **What: Linux/Unix** and derived flavours are the preferred operating system used as the core engine of a lot of network and security devices as well as back office systems.
- **Why:** Mastering Linux/Unix, APIs, and the CLI art will open you to a world of shell scripting, cyber security tools, and other technologies that are essential in order to master the network & security craft.
- **Where to start:** Many flavours are available. I recommend Ubuntu as a starting point as it is friendly to beginners.

I set-up the iCyber-Academy because of the significant lack of skills, that I noticed as I went into companies to help their staff deal better with the technologies they were using to protect their businesses. Unfortunately more often, I observed this skill gap when I went into a client who had suffered a breach and the staff were unsure of how to contain the problem. I realised that despite being strong technicians the staff often struggled to have both a sound and fast reactive grasp of the technologies and tools they were using and the problem was getting worse as more tools being were bought to protect the companies on an ever wider basis.

iCyber-Academy

Today, iCyber-Academy is one of the leading cyber-security training providers in Europe. We provide an environment where elite consultants can learn, gain accreditation, get mentoring, network and open up additional opportunities to get billable work. Over 100 independent security consultants have been trained. The same environment is available to Companies and over 100 companies have been trained, often on-site. Often our courses are delivered through recognised training companies such as Avnet and Arrow.

Our latest development is a 10 month programme (usually a week at a time or a couple of weekends a month) which provides an end-to-end full stack training program. This will allow you IT Security Staff and Consultants to acquire the necessary skills needed to take on any type of cyber-security

messages-steal-sensitive-data-funds-1654696

Security researchers have discovered a mobile malware strain that can intercept users' sensitive SMS messages to steal their banking details and funds. According to Trend Micro researchers, the malware dubbed "FakeBank" has been spotted in several SMS/MMS management software apps and primarily targets victims in Russia and other Russian-speaking countries.

"These advertised SMS management capabilities are turned against the victim. The malware intercepts SMS in a scheme to steal funds from infected users through their mobile banking systems," Trend Micro said in a blog post published on Wednesday (10 January). The researchers have observed the malware targeting customers of numerous Russian financial institutions such as Sberbank, Leto Bank and VTB24 Bank. It has also been spotted in China, Ukraine, Romania and Germany among other countries.

Half Million Impacted by Four Malicious Chrome Extensions

http://www.securityweek.com/half-million-impacted-four-malicious-chrome-extensions

Four malicious Chrome extensions managed to infect over half a million users worldwide, including employees of major organizations, ICEBRG reports.

The extensions were likely used to conduct click fraud and/or search engine optimization (SEO) manipulation, but they could have also been used by threat actors to gain access to corporate networks and user information, the security company warns. The malicious extensions were discovered after observing an unusual spike in outbound traffic volume from a customer workstation to a European VPS provider, ICEBRG reveals. The HTTP traffic was associated with the domain ‘change-request[.]info’ and was generated from a Chrome extension named Change HTTP Request Header. While the extension itself does not contain “any overtly malicious code,” the researchers discovered the combination of “two items of concern that” could result in the injection and execution of arbitrary JavaScript code via the extension.

Attackers Use Microsoft Office Vulnerabilities to Spread Zyklon Malware

https://threatpost.com/attackers-use-microsoft-office-vulnerabilities-to-spread-zyklon-malware/129503/

Spam campaigns delivering Zyklon HTTP malware are attempting to exploit three relatively new Microsoft Office vulnerabilities. The attacks are targeting telecommunications, insurance and financial service firms. According to FireEye researchers who identified the campaigns, attackers are attempting to harvest passwords and cryptocurrency wallet data along with recruiting targeted systems for possible future distributed denial of service attacks. Researchers said attacks begin with spam campaigns delivering malicious

project. Each training session is a combination of theoretical knowledge, practical activities and real life case studies.
After completing the program, you will be able to deploy, implement, and architect Cyber-Security solutions, including products from leading Cyber-Security vendors such as F5 Networks, Clearswift, A10 Networks, Check Point, Juniper, RSA, ProofPoint, etc.
You will also have the opportunity to be part of a community of elite cyber-security experts, that can deliver expert level technical Professional Services at premium rates. The Academy also offers shorter courses and is working toward unveiling for 2018 na online training environment. Our goal is to address the top end technical training needs, whilst many other worthy Government sponsored training initiatives target the entry level training skills.

The Full Stack Security Course

Our end-to-end full stack training program will allow you to acquire the skills needed to take on any type of cyber-security project. Each training session is a combination of theoretical knowledge, practical activities and real life case studies.
The training program is composed of 10 modules that can be taken independently or as part of the full package:
1.The Basics of Applications Security
2.How To Design Secure Networks & Applications
3.Web Applications Firewalls
4.Network Firewalls & IDS/IPS
5.Application Delivery Infrastructure - ADI
6.Global Traffic Management
7.Realtime Content Scanning - ICAP
8.Integrating ICAP & ADC
9.SSL Offloading
10.Designing and Building a Fully Integrated Cyber-Security Platform

After completing the program, you will be able to deploy, implement, and architect Cyber-Security solutions and you will have the opportunity to be part of a community of elite cyber-security experts, that can deliver expert level technical Professional Services at premium rates.
As stated earlier the programme is available through recognised training companies or companies can directly purchase the full stack course for their employees or independent consultants can take advantage of the Academy's membership programme to gain additional networking and mentoring opportunities.

Happy learning!

ZIP archives that contain one of several type DOC files that ultimately exploit one of the three Microsoft Office vulnerabilities.

Hackers cast out 300% more phishing attacks via messages
https://www.cbronline.com/news/hackers-phishing-attacks-messages
There has never been a time when more cybersecurity caution has been required when traversing the online world, with the volume of messages carrying malicious phishing payloads spiking by a massive 300 per cent. Emails and messages are not the only dangerous delivery methods employed by hackers when phishing for unsuspecting users, social media accounts are also being used as vehicles to instigate attacks. Since the third quarter of 2017, a 70 per cent increase in phishing links in social media accounts was recorded by security specialist, Proofpoint, also responsible for noting the massive rise in message based attacks. These statistics were provided by Proofpoint as part of its Q4 Threat Report, in which it also revealed that the Trick banking Trojan accounted for 84 per cent of malicious banking spam.

Phishing for cryptocurrencies: How bitcoins are stolen
https://www.kaspersky.com/blog/crypto-phishing/20765/
The simplest version of cryptocurrency phishing, aka cryptophishing, involves good old-fashioned spam mailings. In this case, such e-mails appear to originate with providers of cryptocurrency-related services — Web wallets, exchanges, and so on. The messages are markedly more detailed and sophisticated than the average phishing e-mail. For example, one might be a security alert saying that someone just tried to sign into your account from such and such address using such and such browser — all you have to do is click the link to check that everything's OK. The potential victim might even have requested such messages on the cryptowallet site, in which case they will notice nothing untoward.

Cisco ASA software is affected by a flaw with 10 out of 10 severity rating. Patch it asap
http://securityaffairs.co/wordpress/68424/security/cisco-asa-critical-flaw.html
Cisco addressed a critical security flaw, tracked as CVE-2018-0101, in Adaptive Security Appliance (ASA) software.
The vulnerability could be exploited by a remote and unauthenticated attacker to execute arbitrary code or trigger a denial-of-service (DoS) condition causing the reload of the system. The vulnerability was discovered by the researcher Cedric Halbronn from NCC Group, he will disclose technical details on February 2 at the Recon Brussels 2018 conference. The flaw resides in the Secure Sockets Layer (SSL) VPN feature implemented by CISCO ASA software.

Switzerland: a land where Data Protection rules become a (paying) real asset for individuals

by Laurent Chrzanovski – Founder and co-editor, Cybersecurity Trends

Following – and even enhancing – European Union's GDPR framework, Switzerland adapted and buffed up its Federal Law on Data Protection.

In most of the European countries, compliance to the GDPR is seen with worry by companies which handle personal data, as the fines in case of data breach will be up to 4% of their yearly incomes. But for the private citizen, GDPR looks like an "after-crash" parachute in case of violation of his/her privacy with, depending of the countries, some ways to receive indemnities from the guilty company or to sue it in courts.

On the contrary, Switzerland – besides adopting the same sanctions and fines for breached data holders – proposed a proactive system to all the inhabitants of the country desiring to anticipate and buff up the protection of their data, through public-private partnerships such as the Swiss Internet Security Alliance.

As a consequence, a whole range of free-of-charge services to citizens has been set up (free hotlines in case of phishing, identity theft, encryption viruses etc.), yet the most visible and interesting effect of this 6-months (r)evolution has been the birth of innumerable cheap and well-thought out "individual/family internet protection" contracts proposed as an additional service by all kind of Swiss Insurance Companies.

A person with Swiss residence can now add to their Civil Responsibility, Car, Home or Health insurance the "Internet Protection" extension, with yearly fees starting as low as 4 CHF (3.2 EUR) and rising to a maximum of 100 CHF (85 EUR) per year according to the coverage the customer desires.

The whole Swiss system is based on an individual compulsory and free-of-charge inscription on the website IDprotect.ch, a service created by I-surance.ch and financed by the insurances fees.

There, each individual – and not his insurance – chooses which data he desires to be protected – personal / intimate pictures, texts, passport/ID card numbers, Credit/Debit card numbers and so on.

The role of IDprotect.ch, placed under very strict Federal rules on data confidentiality, is to scan 24/365 the deep web to see if those data are to be found, meaning that they have been compromised. The customer is then immediately called and advised on the procedures to follow and attitude to adopt.

As on the net everything is about time, the team at IDprotect will immediately start to deal with the most urgent technical and juridical aspects (fraud, identity theft, client's assistant to data recovery in case of crypto-ransomware, direct medical assistance in case of a child or teen in the family is victim of grooming/bullying, a.s.o.).

An amazing element, if we take the mid-level and top-level contracts is that for less than a hundred Euros a year an individual is insured as follows:

1. World coverage
2. Help in eliminating all private data leaked
3. Up to 5000 CHF directly paid to replace the damaged device(s)
4. Up to 1000 CHF for undelivered online purchased goods (min. 200 CHF value)
5. Up to one million CHF (850'000 EUR) for lawyer's costs – free choice of the lawyer –, court costs, forensics costs*
6. Indemnity for direct financial losses (for private professionals) and reputation loss
7. Health expenses unlimited coverage in case of psychological consequences for 5 years
8. 300'000 CHF in case of partial invalidity caused by an attack (blackmailing, etc.)
9. 150'000 CHF to the family in case of death (suicide)

* The list of cases covered is impressive:

- Abusive use of identity
- Abusive use of bank / credit card credentials
- Victim of phishing
- Victim of hacking
- Victim of blackmailing or threatening to the individual or his family
- Victim of sexting, grooming, bullying
- Victim of stolen virtual property: intellectual property, author's rights, trade marks and names registered individually, stealth or unauthorized use of private images or confidential texts, a.s.o.

The most important aspect of the new insurance services proposed in Switzerland is the forecasted ability for individuals to obtain (at their choice) a full protection to fit the possible extent of damages and a constant challenge service (except in the USA or some advanced Asian countries) for Company Insurances.

As an example, a "cyber security" insurance for a company in France or Italy, is still based on the gross incomes of the

contract buyer, is generally very expensive, and covers a maximum of some millions in case of damage, which is far below the real financial consequences of the most recent global attacks. The reason of this "half-blind" system is that neither the insurance companies nor the companies buying insurance have strict and uniform standards to evaluate the resilience of the infrastructures, the employees' capacities in security basic knowledge and the effectiveness of the CISO/CSO department.

The lack of awareness of the majority of the companies' boards forms the base of the compulsory under-evaluation extent of the damages. Security being immature as a whole, national insurances cannot reward companies which do perfectly comply to all NIST / GDPR frameworks with fair yearly fees and very high refunds in case of attack, pushing several sectors (banking, finance, critical infrastructures) to contract, where possible, an overseas insurance company.
Why is this new-born service predicted to have such a shiny future?
There are many simple reasons creating the ecosystem where insurance can engage at a fair price and high refunds without risk, and all of them are met in the 26-Cantons country.

1) Swiss citizens are often mocked as being "over-insured", which is partially true yet has to be seen, not as a fear but as a knowledge of the costs in case of problems. Civil responsibility protection, healthcare insurance, car insurance, home insurance and many more are compulsory and privately-handled. Among them, the only public one, healthcare, became private - under State supervision for fixing the annual raising of fees, (after a popular referendum held in 1996). State-managed insurance programmes are only the loss of job insurance and the invalidity insurance as well as a small pension fund, to be completed with private ones.

2) As a consequence of "everybody being insured" and a general mentality of being collectively responsible of being honest with the insurances, the companies of this sector are fully beneficiary and provide customers several bonuses, which are almost an exclusive Swiss privilege. E.g. we can quote the full refund of broken glass in a ca (no matter the cause: urban violence or simple driving incident), without any "bonus reduction" on the next yearly fee.
Another example is the optional hand-luggage full insurance valid everywhere (bus, train, plane) for less than 50 CHF per year – we were stolen once, and the insurance refunded us in a week not only the full price of the of the photo machine which was inside, but also of the cabin trolley!

3) Being proposed for a very reasonable price as a "plus" to an already contracted - and compulsory by law - healthcare, car or home insurance, the cyber-insurance is ready at a click, benefitting in marketing terms of an already "captive customer" (bonuses) having a long-term relationship with the company.

4) With a knowledge and free choice of "which data to protect" the trust and collaboration between the customer and the insurance is total. Moreover, the insurance platform can use all its assets to scan the net in search of very precise items and reduce at a maximum the duplication of leaked/stolen data when they appear.

5) Without being naïve, several of the services offered are already packed in the compulsory insurances (illnesses, invalidity, death) or in the financial terms most Swiss Banks offer (full credit card data stealth coverage, very limited fee to pay if debit card stolen with PIN, a.s.o.)

Anyway, these new insurances will make some companies (like aggressive ecommerce ones) very careful with Swiss data of unknown provenience or bought on the grey market. The possibility for Swiss citizens to easily benefit from coverage of lawyer and court costs up to one million CHF will give to Swiss citizens the capacity to sue, if needed, a US company in a US court, an action which is financially impossible to any normal European citizen.