GLOBAL CYBER SECURITY CENTER

Newsletter

2018 February

Cyber Security is our mission

editorial

Smartphones, social network the new battleground in our pocket.

Was running 2014 when the hashtag #AllEyesOnISIS appear on the net, this hashtag was not announcing a new movie, but the Iraq invasion. Then was an increasing of sharing video, conversations, and indoctrination, echoing with billions of voices from ISIS.
Social media help ISIS to recruit foreign fighter all over the world, different sources are talking of more than 30.000 people. They use also social media for declaring war against United States, video, tweet, but also the execution of US citizen broadcasted by YouTube and social network. ISIS made also an App that allows their fans to follow everything easily linking social media registering an incredible number of tweets.
The amazing thing was that ISIS build their viral "success" as movies makers and record companies used to advertise the latest movie of Spielberg or the new album of Lady Gaga. Same principle, same *marketing strategy*. Always in 2014 during the Russian annexation of Crimea, the Russia government spent over 19 million dollar on social media operation, as wrote analyst Michael Olloway (https://thestrategybridge.org/search?q=%23WhatIsIO). The goal was to influence international opinion and create an image of a large population supportive of the annexation.
The author of "War in 140 Characters", David Patrikarakos wrote that these new digital platforms are creating new scenario and a new battlefield in people's everyday lives, pushing propaganda via smartphones that are with us 24 hours a day. Going to 2016 in US we may see today as Russia influence operation against the presidential election. They moved from mail hack to a more sophisticated campaign on social networks. It seems also that more than 10.000 Twitter users were targeted with sophisticated malware that once running permit them to take the control of the victim phone and computer. Not only, as FBI is reporting, Russia used robot programs to spread disinformation and amplifying messages and manipulating public opinion.
Algorithms that use mathematical formulas to segment population in group according to defined characteristic like political opinion or religion. Identifying the people that is following these group sending them messages for influence them, deploying provocateurs based on bots altering and influencing the follower behavior.
A new scenario that can influence the course of the elections or the course of a nation's history. To trigger revolts, civil wars, a new war scenario where no armies or nuclear weapons are needed. Nothing new under the sun, history repeats itself, the telegraph was considered an instrument for spreading peace and civilization, but it also became a fundamental tool in the wars that bloodied our planet. And thinking about our elections? The electoral campaign that is going to end passes in part to the network where the groups face each other with Tweet and posts on Facebook. Do you remember something? Have a nice reading…

Enjoy your reading

Nicola Sotira
General Manager GCSEC

events

IDC's Annual Security Conference 2018. Security, risk and compliance; Life after GDPR
Location: London, UK
Date: March 14, 2018
http://www.cvent.com/events/idc-s-annual-uk-security-conference-2018/event-summary-48a484ab6f3a46f6baa55363f17f1637.aspx
Accelerating Digital Business Through Security, Risk & Compliance.
International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy.

Cyber Intelligence Asia 2018
Location: Singapore, Singapore
Date: March 20-22, 2018
http://www.intelligence-sec.com/events/cyber-intelligence-asia-2018
Cybercrimes are constantly becoming an everyday occurrence and the attacks are also sophisticated and unknown causing governments to make sure their cyber defence systems are updated regularly.
Cyber Intelligence Asia will provide you the opportunity to meet with leading cyber security experts from across Asia-Pacific in one place. You will also have the opportunity to network with senior Singapore government and military officials who set their cyber security strategies and plans

Cybersecurity summit Roma 2018
Location: Rome, Italy
Date: March 21, 2018
https://www.theinnovationgroup.it/events/cybersecurity-summit-2018/?lang=it
The objective is to take stock of the state of the art of the commitment of the European Union and of the individual Governments in

in this number

5 Reasons single-password authentication should be banned

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

I use passwords a lot. I have different types of passwords. From strong, mega strong, and paranoid strong. Some I can remember, some I can't – it drives me mad sometimes. Whether you like passwords or not, single-factor authentication (SFA) – also called single-password authentication – remains one of the most common first lines of defense used by various online systems to protect against unauthorized access to applications and data.

Single-password authentication remains one of the most common attack vectors used by cyber-criminals to break into online systems. My view is that single-password authentication should be banned worldwide. All publicly accessible online systems that rely on single-password should be forced to use at least one form of strong multi-factor authentication (MFA). In this article, I cover five reasons why.

The growing threat of phishing, ransomware, and advanced persistent threats (APTs)

With the rapidly growing number of sophisticated cyber-attacks, such as phishing and ransomware, SFA has had its day. One way to fight back against the rise in cyber-attacks is by using strong MFA. It must be widespread and used as the most basic type of authentication mechanism. Unfortunately, many service providers and organizations still rely on SFA as their preferred method of authentication for online systems connected to the internet. This is very bad. Here are five reasons why.

1. Humans are naturally 'lazy' when it comes to passwords

When we are challenged to create a password, we often choose something we can remember easily. That usually leads to a weak password. Using password generators software can help create very strong passwords. However, various online systems still do not enforce strong password policies which means users can get away with creating very weak passwords.

2. Computing power is increasing dramatically

Password-cracking tools are getting more powerful. With the dramatic increase in computing power, these types of tools are now widely used by cyber-criminals. Such tools are used to guess and break passwords quickly using brute force computational algorithms. And with quantum computing this power will increase exponentially, allowing password-cracking tools to break even the strongest password in a short period of time.

3. Some service providers still store unencrypted passwords

We hear in the news every day about various online systems breached and personal information stolen. One such case was LinkedIn. By stealing millions of passwords, cyber-criminals used the password database to develop better tools for cracking passwords much faster.

terms of security and resilience of national critical infrastructures, leading to the discussion table with the institutions and experts of the sector themes such as:
The problems that underlie international collaboration and the realization of the most effective strategies;
Implementation of the standards - NIS Directive, GDPR, international standards;
Information warfare and how to define a common response strategy.

EuroCyber: Are you business-ready for GDPR?
Location: Rome, Italy
Date: May 9–10, 2018
https://skytopstrategies.com/eurocyber-2018-italy/
This conference will convene executives from multinational companies from around the world to address the implementation of GDPR and related compliance performance expectations. The objective of this program is to educate senior level executives on how to effectively achieve GDPR compliance in an environment of complex operational considerations.

news

Scarabey: This ransomware threatens to slowly delete your files every 24 hours until you pay up
http://www.ibtimes.co.uk/scarabey-this-ransomware-threatens-slowly-delete-your-files-every-24-hours-until-you-pay-1658742
A new variant of the malicious Scarab ransomware has been uncovered in the wild that uses a different distribution method and threat to scare victims into paying up. While the original Scarab ransomware was distributed by a massive spam campaign hosted by the Necurs botnet, the new variant dubbed "Scarabey" targets Remote Desktop Protocol connections and is manually dropped on servers and systems.
Discovered in December 2017, researchers at Malwarebytes say the new threat seems to be targeting Russian users. Similar to other ransomware, Scarabey demands a Bitcoin payment from victims after infecting their system and encrypting all files.
According to the researchers, the code between both Scarab and Scarabey are almost "byte-for-byte identical" but do include some notable differences.

Unicode Technique Used to Deliver Cryptomining Malware Through Telegram
https://threatpost.com/venerable-unicode-technique-used-to-deliver-cryptomining-malware-through-telegram/129929/
Attackers are using the time-tested right-to-left override technique to deliver cryptomining malware through the popular Telegram messaging application, say researchers.

4. Password renewals frequency

One way to keep your password safe is by changing it on a regular basis. Various online systems are enforcing this mechanism to strengthen security. However, forcing users to change password at short frequency leads to password fatigue. Unless strict passwords policies are enforced, users may often re-use previous passwords for convenience.

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.

5. Password fatigue

Too many passwords. Too many online systems. Users are feeling the password fatigue. Many organizations are increasingly implementing single-sign-on (SSO) to allow users to login once using a single-password and then gain access to several online systems using a chain of trust. However, if the initial password used to gain access is weak, the overall system is also weakened in the process.

Preventing unauthorized access with strong MFA

In summary, single-password authentication remains one of the most widely used mechanisms to protect various online systems against unauthorized access. Relying on single-password authentication alone is bad practice. I argue that it should be banned completely. All online systems accessible from the internet should be forced to use strong MFA – this will greatly reduce the rapidly growing number of cyber-attacks worldwide.

The right-to-left (RLO) technique uses Unicode to hide malicious file names and trick users into executing what appear to be benign files. It is a tactic that enables malware authors to hide the real name of a malicious executable.

The vulnerability was found by Kaspersky Lab in the Telegram's Windows client in October 2017, according to Alexey Firsh, a security expert at Kaspersky Lab.

Firsh gave the example of the RLO attack in action. For example, hidden in the file name is Unicode that reverses the order of the characters that follow it. So, for example, the malicious JavaScript executable with the name "gnp.js" becomes what appears to be a benign PNG image file "sj.png".

Hackers could obfuscate malware through code signing and SSL certificates

http://www.securityweek.com/half-million-impacted-four-malicious-chrome-extensionhttps://www.scmagazineuk.com/hackers-could-obfuscate-malware-through-code-signing-and-ssl-certificates/article/746258/

Security researchers have discovered that hackers are able to obfuscate malware through code signing and SSL certificates. According to a new report by Recorded Future, researchers have discovered that dark web vendors are offering made to order certificates which are registered using stolen corporate identities.

In a blog post, Andrei Barysevich, Recorded Future's director of Advanced Collection, said that in 2017 security researchers around the world started seeing a sudden increase in code signing certificates being used as a layered obfuscation technique for malicious payload distribution campaign.

Investigations by Recorded Future's Insikt Group found that while the earliest use of stolen code certificates in 2011, it was not until 2015 that code signing certificates became widely available in the criminal underground.

New Saturn Ransomware Actively Infecting Victims

https://www.bleepingcomputer.com/news/security/new-saturn-ransomware-actively-infecting-victims/

A new ransomware was discovered this week by MalwareHunterTeam called Saturn. This ransomware will encrypt the files on a computer and then append the .saturn extension to the file's name. The Saturn Ransomware is being actively distributed, but at this time it is unknown what distribution methods are being used.

When Saturn Ransomware is installed it will check to see if the victim is running in a virtual environment. If it detects that it is running under a virtual machine, it will exit the process. If it does not detect a virtual machine, Saturn will execute the following commands to delete shadow volume copies, disable Windows startup repair, and to clear the Windows backup catalog.

Time to move beyond cyber-fear

by Alison Hanley - Marketing consultant specialising in fintech, cloud, mobile services and cyber-security

There's no shortage of news when it comes to data breaches. Every day we face new headlines where trusted brands and institutions have fallen foul of the fraudsters. And these high-profile incidents are just the tip of the iceberg.

The introduction of Europe's new General Data Protection Regulation (GDPR) next year, which mandates that all data breaches must be reported, will help reveal the true scale of the problem.

While transparency is good, it could also send many organisations into a frenzy of activity where strategy is driven by fear and investment is focused on 'lock-out' technology which creates more friction for users.

This will be exacerbated by lack of positive cyber planning and skills development, which is already a major issue for the UK.

Experts highlight the issues

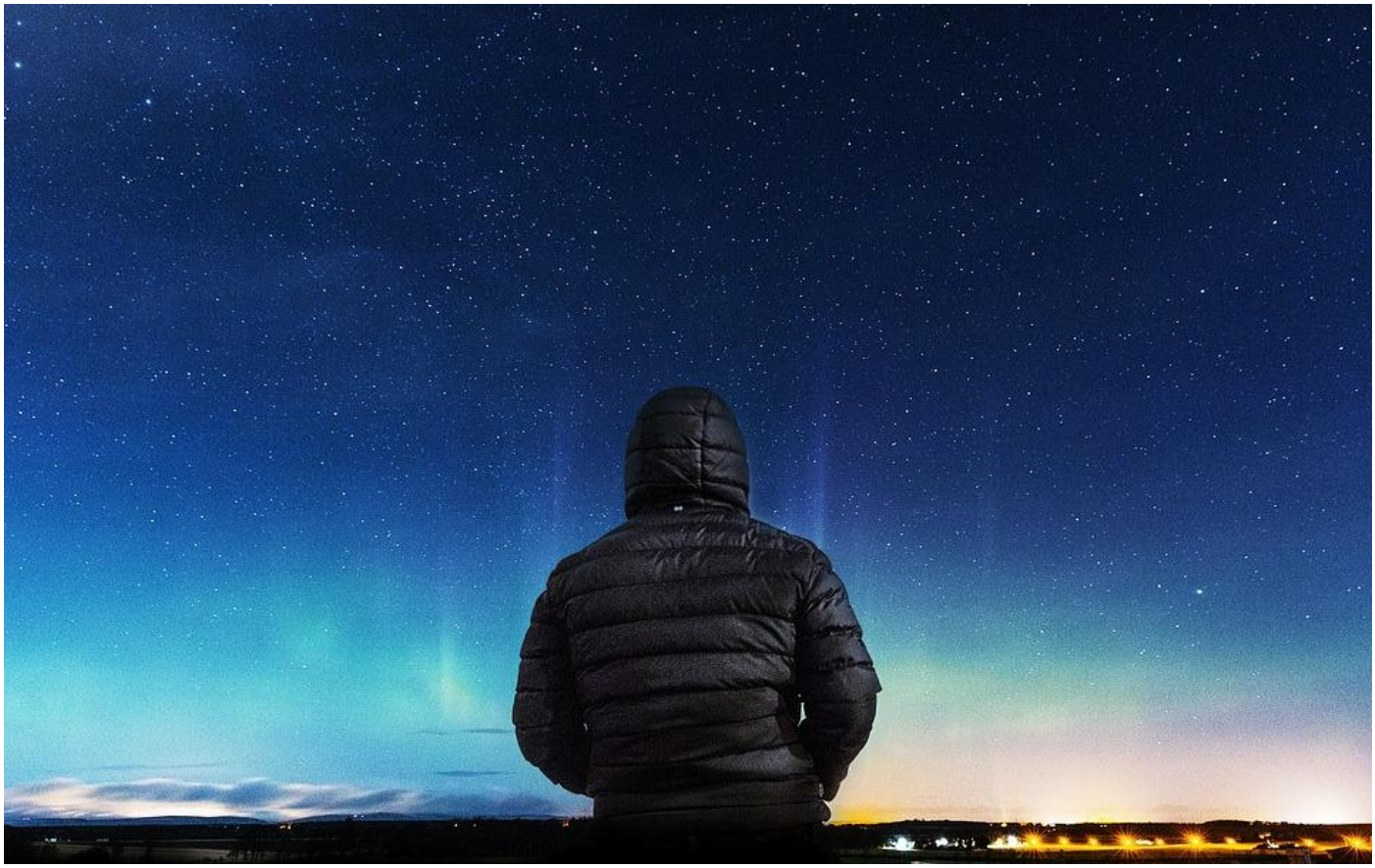
According to a recent iCyber-Security research report. Feedback from 10% of the UK's top independent cyber consultants revealed that fear, poor skills and knee-jerk reaction to breaches are the norm when it comes to safeguarding Britain's digital assets. Not unsurprisingly, it suggests that too many vulnerabilities are still down to poor practice such as weak passwords – a common starting point for many breaches.

Much of this could be down to a failure to invest resource, time and effort into enterprise training on security and user safety and in the underlying shortage of good cyber skills and expertise in the UK. All too often it seems to take an incident of fraud or data loss to escalate cyber-security up the agenda of company Boardroom priorities.

The iCyber-Security study reinforces this by confirming that 43% cyber-consultants believe that training and skills is the biggest cyber challenge facing UK business. A staggering 93% feel there is currently insufficient investment in cyber security. And the same percentage pointed out that cyber-investment is being propelled by 'threat'. Finally, 40% indicated that negative media coverage of breaches, and 30% that a lack of skilled resource was driving cyber-outsourcing.

So, what's going on and where are the majority of the threats coming from?

Well it seems that Application Level and Distributed Denial of Service (DDoS) are deemed the most common forms of attack with 'weak passwords' being the most widespread vulnerability. Looking to the future,40% of cyber security consultants expect to see Ransomware, and 30% Identity Harvesting, become more prominent in the next 2-3 years. With cloud services and connected devices (IoT) becoming the areas most frequently targeted.



Increased regulation and consequence

For many organisations the situation hasn't been helped by the lack of regulation in the industry. Few would argue that more protection is needed for consumers and for businesses. The new EU GDPR regulation, which comes into effect from 25th May 2018, is considered long overdue by some consultants.

However, many businesses, especially SME's are not prepared for this regulatory change and for the new 72-hour breach notification and handling requirements involved. Failure to comply will come at a heavy price – with mammoth fines of up to 4% of annual global turnover. For large and small organisations, this could be a crippling blow when added to the loss of business and reputation.

Taking a positive stance

As our digital world grows, so will the incidence of cyber-crime and the inevitability of breaches. It's completely understandable that UK organisations feel threatened by the scale, complexity and consequences involved in securing their data.

However, it's vital that enterprises don't allow a negative attitude to cyber-investment to exacerbate the situation. It's time to make cyber-investment a 'positive choice' and not one driven purely by reactivity or compliance.

At present 80% of cyber security investment is currently focused on 20% of the threat. There has to be a more considered and thoughtful approach to balance this and to reallocate investment where it can have the biggest impact.

Organisations must ditch their reluctance to talk about their security externally. All too often, specialist help is sought AFTER data has been compromised – when the horse has already bolted! It makes much more sense to assess, plan and remove vulnerabilities BEFORE a breach occurs.

Many cyber-security experts believe that risk could be reduced if they were brought in earlier on, when systems and processes were being designed. This would allow them to optimise infrastructure and investment, make IT more productive and prevent future-risk through technical innovation, best practice and comprehensive cyber security training.

Closing the skills gap

This leads us to the real nub of the issue. The crippling shortage of cyber security professionals that is threatening businesses in the UK, where more than two thirds of companies are already struggling to recruit the levels of staff necessary to defend against major attacks.

Almost half of British businesses say that the skills shortage has a "significant impact" on their customers and has caused breaches of their computer systems. This is symptomatic of the global shortfall of security experts, which is expected to reach 1.2 million by 2020 and increase 20pc to 1.8m by 2022, according to industry association ISC Squared.

It's essential that Britain PLC invests quickly in expanding the pool of accredited cyber security professionals. Fraudsters and cyber criminals have no boundaries, so companies need broader cyber security strategies and better qualified expertise to protect their brands and safeguard their businesses today and tomorrow.

While most businesses have at least some basic technical controls, such as firewalls, patched software and anti-malware programs, few are aware they can be certified for having the full range of controls required.

Nurturing national talent

Even before the recent NHS breach, the UK Government had recognised Cyber-security as a national issue - not just for business but also for our infrastructure.

In February this year, it opened the National Cyber Security Centre (NCSC) to provide a clearer focus in defining the National Cyber Security Council's (NCSC) role in preventing attacks. 12 separate teams from central government are now charged with tackling or preventing potential cyber threats.

In terms of boosting skills, the Government has also teamed up with the British Computer Society to introduce cyber security modules onto computer science degrees, giving an extra 20,000 people skills a year.

At the same time, it has made a £20m investment in a new cyber curriculum, to give thousands of the best and brightest young minds the opportunity to learn the latest cyber security skills alongside secondary school studies through extracurricular clubs. It hopes that these will help identify and inspire future talent to help prepare Britain for the challenges it faces ahead.

In addition, there are now dedicated training facilities for accredited experts to increase their knowledge and expertise.

For example, Thames Valley based iCyber-Academy, supports a broad range of vendor certifications and training programmes as well running regular skills workshops and online training schemes for both in-house cyber-security

professionals and external consultants. It is seeing demand for its courses rise as more businesses, individuals and educational institutions sign-up for skills development.

Rewriting rules from the top

It would be easy for businesses to feel overwhelmed by the threat and aftermath of data breaches. And for staff and customers to feel anxious of the consequences. However, by treating cyber-security as a 'people' issue and not purely as an IT issue, organisations can gain some control.

Through adequate training they can equip their staff to mitigate risk and encourage customers to manage their security settings, passwords, etc more effectively. By adopting a more proactive approach and - not just a reactive response and by broadening out their investment to include specialist independent security consultants as well as IT support then there is no reason why they cannot reduce their vulnerabilities.

Many of these changes must come from the top. That means the C-class needs to take some ownership of the issue and make it an active part of their regular business discussions, encouraging and supporting cyber-security initiatives, creating cross functional teams and empowering employees with suitable resources.

To truly change attitudes to cyber security, 'creating a safer digital world' needs to become a corner stone of how we do business – not as something to be feared, but as something to be embraced, celebrated and invested in by all.