Global Cyber Bi-Weekly Report by INSS February 15, 2020

Editor-in-chief: Gabi Siboni, **Editors:** Gal Perl Finkel, Gal Sapir

Contributors: Simon Tsipis, Yael Elharar, Rachele Buffa, David Murcia Briceño

ISRAEL

Siemens admits: A serious security breach endangers our customers worldwide

Siemens, the German industrial manufacturing company, issued a warning about a serious security breach in the industrial communication protocol Profinet. The breach endangers all customers who have Siemens products and who use the protocol in their operations. "The main and most serious danger is to critical infrastructures, such as electricity companies, energy, transport (railways, public transport, and aviation) as well as hospitals and industrial production systems." The breach was uncovered by researchers at the Israeli cybersecurity company OTORIO. According to OTORIO researchers, this loophole is almost impossible to completely block, which enables exploitation by malicious hackers or accidentally by employees, which can disrupt operation systems and controllers' operation and ultimately immobilize production infrastructure. This is a significant discovery as Siemens is the world's largest manufacturer of industrial components, and its products are installed in thousands of essential and important facilities in Israel and around the world.

https://bit.ly/2SlHCEn

Following the security breach: Likud application procedural testing

A security breach was discovered in the Likud party's Elector app in Israel, causing the party's voter registry to leak, which included private information such as identity numbers, telephone numbers, names, addresses, and political

information of approximately 6.5 million Israeli citizens. Following the leak of personal information from the Likud voter registration, the Justice Department's Privacy Protection Authority opened an investigation on the suspicion of violating the provisions of the Privacy Protection Law and Privacy Protection (Information Security) Regulations and possibly the Election Law. Electoral applications, like Elector, enable "field activists to identify acquaintances and relatives as party supporters and attach them through the party database app" among other actions. "The Protection Authority is working with one of the companies that apparently leaked the information and is working to prevent further information leakage. According to the Protection Authority, parties have a duty to protect the privacy of their voter register in accordance with the Privacy Protection Law and prevent such occurrences. In the event of a breach of the law, a party may bear criminal and civil liability. The Cyber Department of the State Attorney's Office accompanies the Protection Authority in investigating the incident."
https://bit.ly/3btuzrL

Optimove acquires the Israeli company Axonite for millions of dollars

The Israeli hi-tech company Optimove, which develops marketing technologies, has acquired the Israeli company Axonite, which specializes in information streaming. The value of the transaction is estimated at millions of dollars. Axonite's technology enables one to collect and respond in real time to information from multiple systems in combination with automation and artificial intelligence technologies. "The platform developed by the company simplifies the process of building, deploying and running customer-centric, large-scale business applications and high data streaming rates." According to Pini Yakuel, CEO and founder of Optimove, "the acquisition completes our new data infrastructure 'Optidata.' The infrastructure will provide marketing people around the world direct access to their customers' data in real time. In addition to two-way synchronization to any other system or database in the

organization, such as customer retention systems, customer club, finances, and more."

http://tiny.cc/krzwjz

http://tiny.cc/5w0wjz

Oppenheimer: Check Point shares are trading 26 percent below their worth

The Oppenheimer Investment Bank has issued a "high yield" recommendation for the Check Point stock with a target price of US $145 per share while currently trading at US $115 per share given a 12 percent increase in cloud subscription activity. According to the bank, "in the forecast for 2020, Check Point's management expects an estimated US $ billion in revenue." The Bank presents calculations and data that form the basis of its recommendation.

http://tiny.cc/712wjz

UNITED STATES

US says Chinese military stole masses of Americans' data

In 2017 Equifax systems were breached, impacting the personal information of 145 million people. The monumental hack cost the company US $700 million and its reputation. Recently, the US Justice Department faults Beijing, given that four members of the Chinese military have been charged with breaking into the computer networks of the credit reporting agency. The case is the latest American accusation against Chinese hackers suspected of breaching networks of US corporations, including steel manufacturers, a hotel chain, and a health insurer. It comes as the Trump administration has warned against what it sees as the growing political and economic influence of China and efforts by Beijing to collect data for financial and intelligence purposes and to steal scientific research and innovation.

https://bit.ly/2Sfu3WK

https://bit.ly/2w6SsVT

New cybersecurity system protects networks with LIDAR, no not that LiDAR

A team of researchers from Purdue University in Indiana created a new system the enhances mapping out a threat environment—LIDAR—or "lifelong, intelligent, diverse, agile and robust." The valuable tool is used for remote sensing and mapping and features prominently in the awareness tools of self-driving vehicles. Purdue's LIDAR is a kind of architecture for network security. It can adapt to threats, thanks in part to its ability to learn three ways. These include supervised machine learning, where an algorithm looks at unusual features in the system and compares them to known attacks. An unsupervised machine learning component looks through the whole system for anything unusual, not just unusual features that resemble attacks. These two machine-learning components are mediated by a rules-based supervisor. "This is not to be confused with LiDAR, for Light Detection and Ranging, a kind of remote sensing system that uses laser pulses to measure distances from the sensor."
https://bit.ly/2UMle8z

Pentagon weapons tester hones in on cyber tools

According to the annual report published by the Director Operational Test and Evaluation office (DOT&E), the Department of Defense "has bolstered its focus on cyber capabilities pursued by the department through US Cyber Command and its service acquisition executives." It is noteworthy to mention three programs described in the report: the Unified Platform, Joint Cyber Command and Control, and the Persistent Cyber Training Environment. The Unified Platform, run by the Air Force and Joint Cyber Command and Control—which is part of the Joint Cyber Warfighting Architecture—is meant to allow cyber forces to share information, conduct mission planning, and provide the command-and-control tools needed to conduct cyber missions. The Joint Cyber Command and Control will provide joint commanders with enhanced situational awareness and assist in the battle management for cyber forces and missions. The Persistent Cyber Training Environment, run by the Army, is an online client that members of Cyber Command's Cyber Mission

Force can access from anywhere in the world for training purposes and to rehearse missions.

https://bit.ly/2vo9Chz

EUROPE

Huawei: UK 5G concerns a witch hunt says Chinese ambassador

China's Ambassador to the United Kingdom, Liu Xiaoming, defines the Tory party opposition to the initiative conceding the UK 5G coverage to Huawei "a witch hunt." The Conservatives explain their overt dissent declaring that they are determined to give the national critical infrastructure to the "trusted vendors" only, as they are businesses originating from states which recognize as fundamental principles "fair market competition, rule of law, respect human rights, data privacy and non-coercive government agencies." In contrast, engaging with companies whose states do not reach such standards (high-risk sellers) represent a serious threat to the national security, airing a resistance against the prime minister. For these reasons, the restrictive regime imposes on the Chinese company its exclusion from zones sensitive the national security, such as "military bases and nuclear sites," in addition to the 35 percent concession. However, Ambassador Liu defends Huawei, arguing that the company is independent from the Chinese government, and it has the capacity to satisfy Boris Jonson's expectation to get the 5G network in the United Kingdom within five years. He also disapproves of the government's limiting Huawei's share to 35 percent as it breaches the tenet of a free economy.

https://bbc.in/2UKeVlU

National Prosecuting Authority partners Russia, Italy for cyber forensics

A few days ago, Kumbirai Hodzi, the prosecutor-general of the National Prosecuting Authority (NPA) announced that a multilateral agreement of

collaboration has been signed between Zimbabwe and Italy, Russia, and other European countries, in order to link the law enforcement mechanism with cyber forensics. The majority of the crimes of corruption leverages the shortcomings of the national justice system, thanks to its high sophistication and cyber capacity, often resulting in a de facto impunity. The awareness of this novel form that the criminal organizations are taking is a necessary step in order to guarantee an adaptable and resilient legal order, which is actually able to counter crimes and bring the culprits to the justice. In Mr. Hodzi's view, the inherent flaws of the NPA are overcome by editing the current national law accordingly and adopting ad hoc training programs provided by the foreign authorities.
https://bit.ly/3bpeN14

RUSSIA

Russia planning to build powerful new supercomputers after seeing its technology lag behind United States and China

Russia's President Vladimir Putin admits that Russia lags behind the United States and China in cyber capabilities and announced that "multiple new supercomputers may soon be installed across the country." According to Putin, plans are already in motion to expand a high-tech network of supercomputers and data centers that would no longer be limited to the capital city of Moscow. Russia has three out of 500 super-computer systems in the world, compared to China (228) and the United States (117). Two of the country's top supercomputers, Lomonosov-2 and Lomonosov, are housed at Moscow State University. The third is linked to a computing center of the Russian Federal Service for Hydrometeorology and Environmental Monitoring.
http://bit.ly/37dsq08

Anti-Putin blogger has throat slit in a hotel room after vocally opposing the Russian president

Allegedly, a Russian political hit squad is running amok in Europe to hunt down any anti-establishment voices in hiding. This includes internet bloggers and activists. One of Putin's critics was found with his throat slit in what police are calling a "politically motivated" assassination in a French hotel. Imran Aliev has been a strong critic of Putin and Chechen leader Ramzan Kadyrov on his popular blog and YouTube accounts for years, working under the pseudonyms of "Mansur Stariy" or "Old Mansur." This already provides a clearer picture of the extent of Putin's activities outside of Russia, which, in addition to tens or maybe hundreds of cybercriminal hackers scattered around the world attacking foreign states, Russia engages in political assassinations of defected Russian security and military officers, like Skripal, Khangoshvili, and Litvinenko, and is now targeting and killing internet activists and bloggers.

https://fxn.ws/2Hiq8lW

Russia engaging in "information warfare" ahead of 2020 election, FBI chief warns

FBI Director Christopher Wray has warned that Russia is engaged in "information warfare" heading into the 2020 presidential elections. Wray said, however, that the law enforcement has not yet seen any ongoing efforts by Russia to target America's election infrastructure. According to the head of the FBI, as in 2016, Russia is relying on a covert social media campaign aimed at dividing the American public's opinion and sowing discord. That effort, which involves fictional personas and accounts, bots, social media postings, and disinformation, may have an election-year uptick but is also a round-the-clock threat that is, in some ways, more difficult to combat than an election system direct hack.

http://bit.ly/2vm9NtD

Russian authorities approved a bill to block dangerous correspondence

A new Russian law will enable Russian law enforcement agencies to block what it considers as "threatening" or "dangerous" email correspondence between internet users in Russia. The initiative, introduced in October proposes to compel email postal service operators to block user's ability, at the request of the authorized federal body, to send electronic messages if the user disseminates information considered dangerous or prohibited in Russia.
http://bit.ly/2wbIcf9

APAC

China launches coronavirus "close contact detector" app

The close contact detector is an application created by the Chinese government and the China Electronics Technology Group Corporation, with the support of the medical and transport authorities in order to ascertain the users' risk of transmitting the coronavirus even in the absence of symptoms. Considering that this app follows the identification of the smartphone's owner, it reflects the commitment of the Chinese government to control and monitor its citizens. However, lawyer Carolyn Bigg does not think that this app raises such perplexities as the large use of sensitive data by the computer network system represents a health necessity for the entire population and nation.
https://bbc.in/38gs0Y4

What should be in Australia's next cyber security strategy

On September 5, 2019 Minister for Home Affairs Peter Dutton released a consultation document on Australia's 2020 Cyber Security Strategy where he warned the entire society outright that the threat has dramatically evolved. The paper at issue highlights the relevant advancements in view of the Cyber Security Strategy set out in 2016, including the opening of a centralized authority responsible for cyber security issues; the fostering of a multilayer approach joining companies, governments, and academia; and the foundation of two proactive services tasked with providing assistance and technical

advice in response to cyber incident. Furthermore, the document stresses the frontline role of the government in adopting an actual cybersecurity action aimed at protecting Australian businesses in the critical infrastructure field. Nonetheless, Dutton feels the necessity to undertake a resilient strategy to enhance the security of business and the community as cyberattacks cost companies annually up to 29 billion Australian dollars. The Australian Signals Directorate's Australian Cyber Security Center (ACSC) has announced in the past months malicious cyber activity targeting businesses as well as users through the exploitation of critical vulnerabilities of some computer network systems. The advisor Peter Sandilands illustrates the serious discrepancy "of security awareness and capability" among companies in several industrial sectors where, unlike a few financial corporations, small companies are significantly exposed to cyber threats due to the lack of an internal protection and response mechanism. For a more secure cyberspace, it is suggested to execute operative actions for mitigating cyber events (the so-called "Essential Eight") and adopt the British pattern.

http://bit.ly/2uDaK0x
http://bit.ly/3bsd0sb
http://bit.ly/2Swt8Ae
http://bit.ly/2vqrJU8
http://bit.ly/39hL34u
http://bit.ly/38jjZBR
http://bit.ly/2OKKJn7
http://bit.ly/37eFXEM

Scammers are trying to exploit coronavirus concerns to breach companies

Researchers from the email security firm Proofpoint uncovered a series of phishing attempts targeting businesses in sectors of manufacturing, transportation, and finance that are vulnerable to trade disruptions because of the coronavirus. "Hackers are preying upon fears about the new coronavirus from China by sending companies malicious emails cloaked as warnings

about the economic repercussions that could occur as the illness spreads." An email subject line reads, "Coronavirus – Brief note for the shipping industry," followed by instructions to download a Microsoft Word document encouraging more information. According to Proofpoint, the hackers attributed to the phishing attempts are attempting to exploit a vulnerability that is more than two years old, referred to as CVE-2017-11882.
https://bit.ly/2tMLOTV

China-linked hackers have targeted Malaysian government, officials warn

The Malaysian Computer Emergency Response Team reportedly have observed an increase in the number of attacks and victims in a campaign against Malaysian government officials. Private researchers have linked the hacking group that is targeting the Malaysian government with Chinese interests. The campaign is aimed apparently in a data-stealing espionage campaign. The hackers have targeted government-backed projects relating to proposals, shipping information, and private sector reports. Evidence suggests the hackers could be the state-sponsored group APT40, who are utilizing a pair of old vulnerabilities in Microsoft products, dating back to 2014, to compromise their targets.
https://bit.ly/39rCeF8

MIDDLE EAST

Why the Iranian cyberthreat has become more dynamic

Following the drone strike the killed Iran's Maj. Gen. Qassem Soleimani in early January, one top military leader said a retaliatory cyberthreat has become more dynamic. Gregg Kendrick, executive director of Marine Corps Forces Cyberspace Command, said that the Iranian regime will likely have to demonstrate to their people that they are still doing something for the drone strike, even if externally they deny any operations. The Iranians will also likely need to help their economy, Kendrick said at a recent event hosted by the

Institute for Critical Infrastructure Technology. This means they will likely target the energy sector to drive up the price of oil to help their illicit oil sales. https://bit.ly/38UjXY

Security Professionals Association (SPA) for SIRA highlights Expo 2020 security at First General Assembly

The Security Professionals Association (SPA) for the Security Industry Regulatory Agency (SIRA) has emphasized the crucial role of safety and security in major events like the World Expo in Dubai before more than 400 members who recently convened for its first General Assembly. With less than a year to complete, a significant amount of visitors from 192 participating countries is expected to descend upon the country across a period of six months, putting Dubai and the UAE in the limelight as they host the first World Fair to ever be held in the Middle East, Africa, and South Asia region. Thus, the delivery of a safe and secure World Expo is of utmost importance, and this can be achieved by implementing a series of programs, workshops, and training sessions to the more than 50,000 security professionals in the UAE.
https://www.securitymiddleeastmag.com/security-professionals-association-spa-for-sira-highlights-expo-2020-security-at-first-general-assembly/

National and cyber security industry set for double digit growth across the MEA region

Demand for national and cybersecurity solutions continues to grow, both regionally and globally, driven by geopolitical tensions and the increasing range and sophistication of cyberattacks. The UAE, in particular, invests significantly to defend itself as it proceeds with its strategy to build a knowledge-based economy while diversifying its economy away from oil. As a strong step in this direction, Abu Dhabi recently set up a new defense group called Edge with the aim to rapidly develop new systems to deal with threats by militant groups and armies. One of the prime directives of Edge is to

rapidly introduce new products into the defense market. These are aimed at addressing key concerns, through existing commercial technologies and a streamlined prototyping process, all of which will be showcased at the 2020 edition of the International Exhibition of National Security Resilience (ISNR Abu Dhabi). It is co-organized with the UAE's Ministry of Interior, with the intention of bringing the national and cybersecurity communities together to accelerate public-private collaboration for a safer connected world. According to Kaspersky, there were more than 150 million malware attacks in the Middle East, Turkey, Africa region in the first quarter of 2019, a growth of 108 percent from the previous year. In addition, according to the 2019 Official Annual Cybercrime Report, damage related to cybercrime is projected to hit US $6 trillion annually by 2021.

https://www.isnrabudhabi.com/industry-news/national-and-cyber-security-industry-set-for-double-digit-growth-across-the-mea-region

LATIN AMERICA & CARIBBEAN

Cybersecurity as a business, better than selling weapons

Nowadays, cybersecurity is a relevant topic in Chile. The digital revolution has long impacted the structure and costs of defense in all countries. Speed, technological complexity, and networks are the obstacles that cybersecurity must face. A voluminous use of hardware and software for defense is central, whether to coordinate resources, execute remote control, or to control operations and theaters, with an essential minimum of regular human resources. This has also reached the profile and volume of Chile's armed forces. The emergence and increase of fortune firms that act as subcontractors in conflicts, without a predefined national flag, more than double the volume of national forces in theaters of operations. The new profile of the defense actors has changed. One of these changes corresponds to the profile of defense providers, which are increasingly participating in their offers with larger digital components, in relation to weapons systems.

https://tinyurl.com/sdwgyf5

Minister Gustavo Montalvo is appointed to chair the World Summit of the Information Society

Minister of the Presidency Gustavo Montalvo was elected to chair the World Summit of the Information Society (WSIS), the largest annual meeting of the community of information and communication technologies (ICT) for development, which will be held in Geneva, Switzerland from April 6 to 9 this year. Minister Montalvo will be the first Latin American to chief this annual international meeting that emerged through a resolution of the UN General Assembly in 2001. The international forum is expected to engage more than 3,000 people linked to information technologies from 60 countries, including around 200 ministers, ambassadors, heads of international organizations, regulatory authorities, industry leaders, high-level representatives of civil society, and the academy. In a resolution of 2015, the United Nations recognized the importance of ICT in the realization of the 2030 Agenda for Sustainable Development while underlining that technologies can facilitate progress in relation to the 17 economic, social, and environmental objectives set out in that agenda.

https://tinyurl.com/rk5ug66

EY México inaugurates the Cybersecurity Operations Center in Querétaro

EY México, a business advisory services firm, has opened its Cybersecurity Operations Center (CyberSOC) in the city of Querétaro, with the aim of providing its clients with cybersecurity strategies that will allow them to adapt to the changing environments and scenarios of digital transformation. With this center of innovation, the company wants to expand the area of vulnerable attacks by cyber criminals, which must be proactively addressed. There are several computer threats affecting Mexico, including cryptojacking, vulnerability exploitation, and malware. The CyberSOC EY Querétaro has a team of professionals with extensive experience dedicated to managing the

needs of each client, in a space of 432 square meters of real time monitoring area and with the capacity for 120 professionals.

https://tinyurl.com/qrqp7la