VOL 2 (2018) ISSUE 1

EUROPEAN CYBERSECURITY MARKET

RESEARCH, INNOVATION, INVESTMENT

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY MARKET

RESEARCH, INNOVATION, INVESTMENT

European Cybersecurity Market is a new publication designed to promote innovative solutions and tools in the field of cybersecurity. In order to raise awareness and increase cooperation in the developing digital economy, this periodical will be openly distributed to all interested parties and stakeholders.

ISSN: 2543-7259

European Cybersecurity Market is a quarterly publication.

THE KOSCIUSZKO INSTITUTE

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków, Poland

Phone: 00 48 12 632 97 24
E-mail: robert.siudak@ik.org.pl

www.ik.org.pl
www.cybersechub.eu

CO-FINANCED BY

European Funds
Regional Programme

KRAKÓW REGION
MAŁOPOLSKA

European Union
European Regional Development Fund

FOREWORD

ROBERT SIUDAK
Chief Editor of European Cybersecurity Market
CYBERSEC HUB Project Manager
Research Fellow of the Kosciuszko Institute, Poland

In the Global Risks Report 2018 published by the World Economic Forum, cyberattacks have been ranked as the most challenging technological problem we are going to face. The only other risks comparable to them were associated with environmental factors such as extreme weather events and natural disasters. Indeed, various studies suggest that a successful attack on a single cloud provider could cause between USD 50 to 120 billion in economic damage, an amount comparable to the losses caused by Hurricane Sandy or Katrina. The report also shows that entrepreneurs, more than any other social group, are acutely aware of humanity entering the era of cyber-dependency in which the digital frontier will determine our welfare and success. Cyberattacks are recognised as the risk of greatest concern to doing business in North America and the East Asia/Pacific region, ahead of such traditional factors as financial crises, assets bubble or even terrorist attacks.

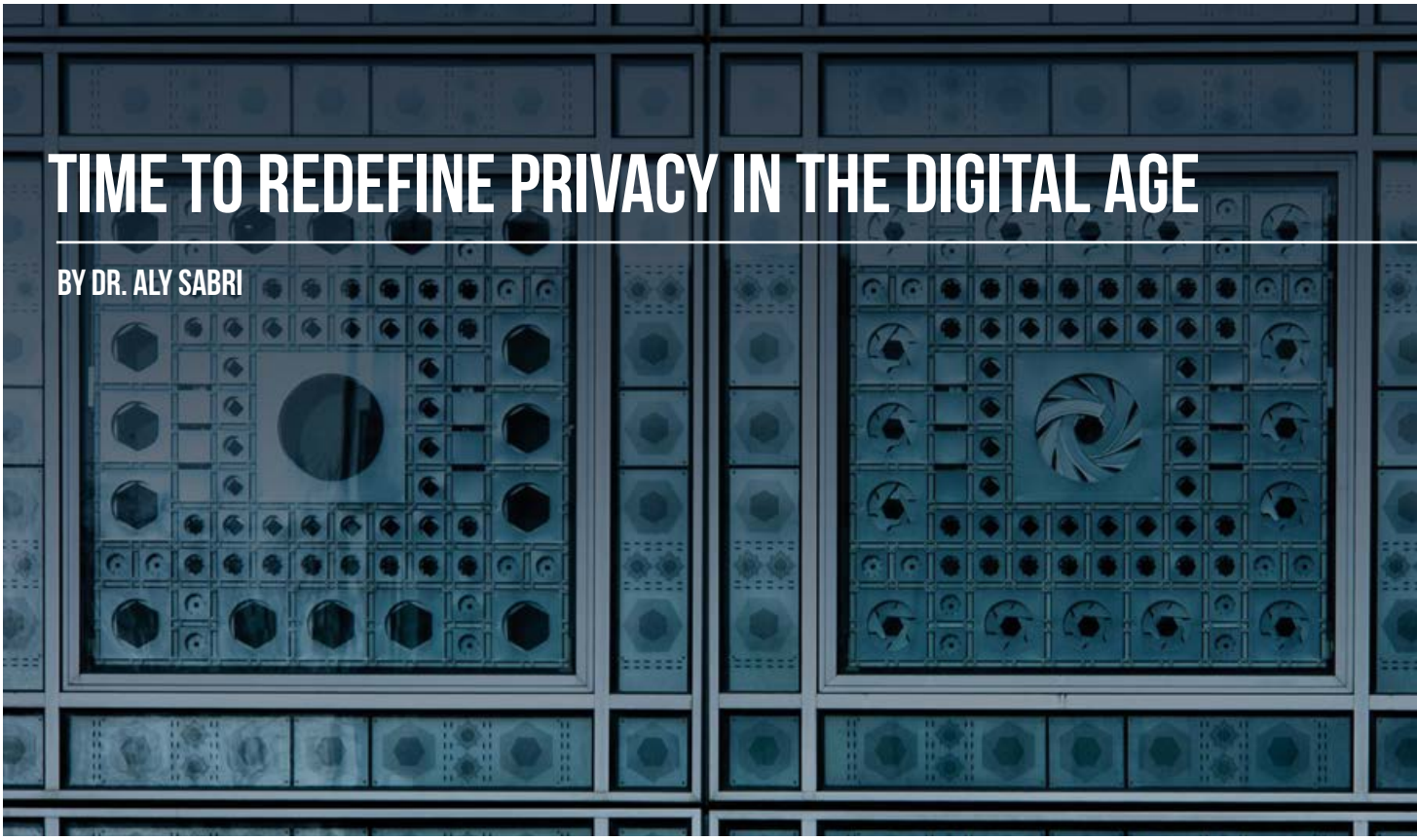
That is the big picture, but at a micro level, things do not appear to be much different. Looking at our private and business lives, we see that year by year we multiply the points of failures in our systems. Only last year, the number of connected devices surged to 8.4 billion, exceeding human population. And this is only the beginning. By 2020, we expect 20 billion Internet-connected machines. Are we going to trust them? What is the remedy for trust in the digital age?

This issue of European Cybersecurity Market provides you with insights into possible solutions that are already on the table. Regulation-driven development of certain technologies and business models is exemplified in the influence of the General Data Protection Regulation (GDPR) on microservices and the rise of customer-orientated privacy laws. On the other hand, the French set an example for (a successful) public-private cooperation focused on stimulating the cybersecurity market. Last but not least, the role of innovative, fresh technological approaches is given in the account of the Startup Pitch Deck Contest which took place during the European Cybersecurity Forum – CYBERSEC 2017.

I hope the articles you find on the following pages will make interesting and stimulating reading. Let the trust prevail!

Robert Siudak

CONTENTS



TIME TO REDEFINE PRIVACY IN THE DIGITAL AGE

BY DR. ALY SABRI

With the digital revolution transforming our lives, the concepts for privacy, data governance, and security seem to lag behind. Increasing user awareness and impending stringent legislation challenge us to rethink and redesign our current practices.

The Current Situation in Privacy and Data Governance

With 4.9 billion users of mobile phones and 8.4 billion connected devices[1], there are more sensors around us than humans on this planet. Tracking is omnipresent. Regardless of whether we are using mobile devices, publishing posts on social media, or driving our car – all our actions are being recorded and processed by analytics tools to gain insight into us as customers. Common motivations vary from the desire to enhance user experience to improving services and products and thereby optimising convenience. With the propagation of the Internet of Things, data gathering is bound to affect our daily lives and headlines like "Connected Teddy Bears Leaked Kids Voices Online" are going to make the future look a bit scary.

All these data are produced by consumers and then stored on corporate servers of the respective provider. This happens formally with the user consent; however, the only true choice the user has is either to "accept or abort". Terms and conditions legalise all data handling and analytics in the present and the future. The problem with these policies is that they are vague, making it completely impossible for the user to foresee the scope and the content of their consent. The extent to which database administrators can access personal data is a hot topic of ethical consideration and legality. Phenomena like the privacy paradox where users state to be concerned about their privacy but behave as if they are not[2], are still common; however, privacy leaks and violations are only the tip of the iceberg, but they are enough to raise user and political awareness.

[1] www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/

[2] https://en.wikipedia.org/wiki/Privacy#Privacy_paradox

To sum up, companies are sweeping up vast quantities of data about consumers' activities and the control over your privacy is de facto in the hands of service providers who are legally covered by terms and conditions the user has to accept in order to use their services. A legitimate question that arises is whether this is a practicable and smart way to deal with the issue – especially when we are observing growing user awareness and stringent legislation about personal data.

Trends in User Behaviour and Legislative Changes

Times when users were indifferently and thoughtlessly using digital services are long gone. "Consumers are aware that they are under surveillance – even though they may be poorly informed about the specific type of data collected about them." According to a study, "97% of the surveyed people expressed the concern that businesses and government might misuse their data. Privacy issues ranked high with 80% of Germans and 72% of Americans are reluctant to share information.[3]"

These results show a growing concern about data usage by third parties and the wish to maintain privacy whilst living in the now with all the conveniences our modern digital life can offer. At the same time, customer expectations are growing: What do I get in return for my data? Is the achieved convenience or service sufficient?

The strict European law serves as a model for personal data protection legislation in other countries.

On the other hand, personal data protection legislation becomes significantly more stringent and consumer friendly. When in 2014 Germany stopped Google violating its Federal Data Protection Act, this was a kind of a landmark for Europe and the rest of the world. The strict European law serves as a model for personal data protection legislation in other countries. The common denominator is to put users back in control and governance of their data currently being in the hands of companies.

The problem with legislation is that it generally lags behind, being a consequence of societal developments. Even so, the General Data Protection Regulation (GDPR) of the European Union is hanging like a sword of Damocles over all businesses devouring vast amounts of money and jeopardising common business models of multibillion companies.

Are Current Business Models in Danger?

A common strategy to conform to the GDPR is to adjust the terms and conditions of the corporation and to build into applications more "accept" buttons to ensure legal compliance. Behind the scenes, however, no or marginal changes are implemented. These actions may keep firms legally out of trouble, but will it be really enough for the future?

Studies show that consumer trust is key for their willingness to share and unlock personal data with service providers. And companies have been taking action to deliver to customers the in-kind value in return for their personal data to gain trust[4]. This strategy proved sound for years; however, the term "convenience trap" is spreading around, making customers ask themselves what they are doing wrong if they still cannot regain control over their data.

In a European Paper issued by Michael Friedewald, seven different types of privacy are distinguished, among them the privacy of data and image which stipulates "that personal data is not automatically available to other individuals or organizations and that the owner of the data has a substantial degree of control over that data and its use"[5]

In our opinion, it will not be sufficient to make legally required changes to terms and conditions and to design smart, value-adding mechanisms to satisfy consumers' expectations for privacy and data control in the future. True data governance in the customer's hand will be the competitive advantage of the future. Terms like "privacy by design" and "privacy by default" have to be lived by the management boards of companies. Paying lip service to it will not last in the future to maintain the customer trust.

[3] Timothy Morey, *Customer Data: Designing for Transparency and Trust*, *Harvard Business Review*, May 2015.

[4] Columbia Business School, *What is the future of data sharing*, October 2015.

[5] Michael Friedewald, *Seven Types of Privacy*, 2013, p. 5.

Current business models do not have to be in danger. This "renewed" need for privacy and governance demanded by customers and law can be viewed as a chance to redefine the notion of privacy for the benefit of all parties involved.

A New Definition of Privacy

Not trying to turn back the wheel of time, let us have a look at how things were before digitalization – to gain some inspiration and to incorporate some ideas into our digital lives today. Before human lives turned digital, we disseminated information by the word of mouth and later with the invention of writing and papyrus – on paper. When an individual was in physical possession of information within its personal private household, no one else could possibly have access to it. The information was under the true and sole governance of the owner. Copying and sharing of information was still possible, but it required more effort and therefore was limited to a far smaller group of recipients.

This "renewed" need for privacy and governance demanded by customers and law can be viewed as a chance to redefine the notion of privacy for the benefit of all parties involved.

This is where trust comes into play. Trust is defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the truster, irrespective of the ability to control or monitor that other party."[6]

As per this definition, it becomes obvious that in the non-digital era, it was much more conceivable and realistic to rely on trust since the number of people having access to one's personal information was much smaller, whereas today, with just a few keystrokes, vast amounts of personal data are available to a worldwide audience, or at least to a significant number of companies, administrators or personality profilers.

The consequence, in our opinion, is that privacy in the digital age has to be redefined to make trust become as controllable and conceivable as it was before, when information was shared on an analogue basis only.

In those days, trust was gained through personal relationships and bestowed on a friend or a person known to the truster. In the digital age, giving away data to hundreds of people with just one keystroke seems normal for users. This data is copied from users' devices to other servers, falling off the radar of the original creator and owner of this particular data element. For the recipients to share this content with further "friends" is again one click away and so a cascading spread of this data begins. Trust in this case becomes obsolete to control one's data. Apart from this behavioural change, currently there is not only the person we put trust in; we also heavily rely on the infrastructure's capabilities to protect our data. We often fail to consider that any kind of software-driven infrastructure will have inherent errors or weaknesses that may compromise the safety of our data. The process of copying makes it even worse: the more often data is copied, the more software systems are involved, and thus the probability for the data becoming completely public increases significantly.

We also heavily rely on the infrastructure's capabilities to protect our data.

A common example of this is email. Email providers do inform their clients to use encrypted, secure access to the mail infrastructure as otherwise user credentials may easily be spied out by a hostile party. The low rate of users employing secure email encryption with tools such as WinPG (heavily funded by the European Union to finally make secure email easily available to everybody) still shows a lack of awareness that the mailing infrastructure will send messages between mailing servers using completely unencrypted protocols. Anyone with access to any of the servers involved, or the transmission backbones, can intercept all of that communication. This equally applies to cloud storage or social media platforms where the provider has full access to the uploaded data.

[6] Mayer, et al., *An integrative model of organizational trust*, 1995, p. 712.

In summary, what is required from digital privacy and trust? What should be the goal?

- First of all, in order to bring back control over data, copying should be abandoned altogether. To still be able to share data with others, it should be enough for data to be referenced only, resulting in a single source of truth for this data. This will help the user and the owner of the data restore full governance over all data at any point in time, from the generation of the data element in the particular source to its ultimate expiration or deletion. Obviously, a recipient of such a reference (the trustee) could still copy data onto his or her own devices, thus putting it beyond reach of the original owner. However, this could be dealt with as abuse of trust, something also known from the analogue world.
- Second, since the infrastructure will still remain in a black box that is highly unreliable, it should only deal with encrypted data. The client-side encryption is a solution which enables the user to trust only the client which is under her/his control.
- Third, and this is in line with the GDPR, data owners should be able to determine on a fine-grained level which data is accessible for whom and for what purpose, and where the red line is.

Once these changes are in place, the users will be back in control of their data with no trust required to be put in neither the service provider handling the data, nor the infrastructure. At the same time, the data will be encrypted and therefore safe against attacks.

Olmogo: a Potential Ultimate Solution

olmogo

The system we consider a solution for the privacy problem described above is called "olmogo". Within olmogo, data elements – called mogos – can be stored using full client-side encryption. Practically, there are no size limitations for data elements; anything from small tracking data to full videos can be stored.

Each and every mogo has a unique URL by which it can be referenced, and a set of encrypted keys through which applicable users can access its content. By adding new or deleting existing access keys, the owner can grant or withdraw access rights for third parties. Unlike other solutions, these keys do not just document who should see what, but actually physically restrict access since without the key, data cannot be decrypted.

To minimise side-channel effects of sniffing software in the transmission infrastructure, a lot of effort is being put into separating data packets and scattering partial information among different servers. User profiles containing the relationships between users are kept apart from the indexing infrastructure storing relationships between mogos and the access keys along with (encrypted) metadata of the content, which, in turn, is separated from the actual data stored.

Mogos can be stored by a third party on behalf of their owner. The creator, the owner, and the storage provider are handled separately. Thus, a company could store the GDPR relevant information on behalf of the data owner, allowing them to fully look into what kind of data was acquired as well as delete or withdraw access rights. Thus, a company using olmogo for storing sensitive information – either as a stand-alone or an additional layer in existing solutions – would automatically comply with the GDPR.

One of the weaknesses of using secure encryption based on a private-public key infrastructure is the protection of the private key. Usually this protection is only as safe as the passphrase used to protect it; once lost, the key cannot be recovered, and without it, all previously encrypted data can no longer be accessed. For this major usability issue, olmogo offers an effective solution by scattering the actual key content over several locations and using a secure protocol to restore it when needed. The actual implementation takes care that key particles stored on each user's end device are distinct from one another, so that even if a device is lost or the passphrase security is compromised, user content can still be protected by deleting all key particles for the lost device and setting a new passphrase.

As fully encrypted content creates a lot of overhead for processing or searching the actual content, we have developed a concept of technical agents within olmogo. Agents can be granted rights just as normal persons, and they can process data to which they have access. Use cases could involve indexing of encrypted data, full text searches, or the use of data by third parties. Unlike in current systems, by administering the access rights of an agent, users can explicitly opt in or opt out of certain usage of their data.

Obviously, creating yet another system in which data can be shared among users might create a burden for those users who would like to stay with their old platforms or social networks. By using the concept of an agent, mogos can also be shared with external infrastructure, allowing, for example, a social network agent with access rights to post the mogo's content on the user's social network account.

To summarise, olmogo offers a secure one-stop-shop for the governance of stored data. By using the concept of an agent, data can be interfaced with current systems, giving users control of what kind of data was shared, even on multiple social platforms. Offering innovative yet secure ways to store the private key reduces the burden of the key management to a minimum. ■

Figure 1. Olmogo Architecture. Source: own compilation

ABOUT THE AUTHOR:

Dr. Aly Sabri is the CEO of the olmogo AG based in Baar, Switzerland. Still in his medical studies in Oxford and Harvard he developed an EPR (electronic patient record) for hospitals. After growing his company to a market leader in Europe he sold his shares to GE Medical Systems. Dr. Sabri´s special interests are innovative software solutions and neuroscience. Over the last two years he and his partner Dr. Schulz invented olmogo - a privacy and data governance solution for corporations as well as consumers.

STARTUP PITCH DECK CONTEST CYBERSEC 2017

BY AGATA WELCHAR,
the Kościuszko Institute

During the contest, Pawel Bogdanov and Ewa Abel comment on one of the startups' pitches.

Startup Pitch Deck Contest, a competition for the best startups in Central and Eastern Europe was held during the 3rd European Cybersecurity Forum – CYBERSEC 2017.

It was an unmissable opportunity for startups in this part of Europe to present their cybersecurity solutions. Young entrepreneurs had a chance to introduce their innovative products to a wider audience and the jury panel including Ewa Abel from European Investment Fund, Debneel Mukherjee from Decacorn Capital, Pawel Bogdanov from Almaz Capital and Bruno Ferreira representing Alior Bank. Each of the 15 short-listed startups had 3 minutes to present their Pitch Deck. Below we present profiles of the participants.

After a fierce debate, the jury selected the winner. The first prize went to **GreyCortex**, a Czech company that employed AI, machine learning and data mining to develop MENDEL Analyst – their flagship solution to analyse network traffic. It helps detect cyber threats, protect data and trade secrets. **VoicePIN.com**, a Krakow-based startup collaborating with CYBERSEC HUB came second in the competition. Using biometrics, the company created an innovative voice authentication system. It is a safe method of identification

without the necessity to remember complicated passwords and login details. Armenian Skycryptor – **BeSafe** snatched third place. Their flagship product BeSafe IO is encryption software enabling data protection, control and analysis irrespective of location and the data sharing method. Being integrated with Dropbox, Slack, and Google Drive, BeSafe IO enables complex and encrypted collaboration in the cloud.

Although there could only be one winner, overall the contest was at a very high level and all participants presented very interesting solutions. **Cyberus Labs** developed CYBERUS KEY, a modern tool for passwordless login. In order to access their account online, the user needs to activate the Cyberus Key mobile app on their smartphone to enable them to log into their bank or e-commerce account on their laptop in just one click. **PHONEID** presented another interesting authentication solution. It is a SaaS model service that offers secure and easy authentication of a user by means of a mobile phone, even without Internet access. It is a method that enables uniform authentication across all channels of communication with the customer, including websites, mobile apps, call centres or physical touch points. Ukraine was represented by **Security System Group**, a company offering a wide array of cybersecurity products and services. One of them is Kryptos, a unique messenger designed to ensure a secure and practical means of communication between users who process sensitive data.

Specfile is another Polish offering in the cybersecurity market. It is an app that encrypts files and allows them to be shared with specific people. Encryption also enables safe data storage online (on cloud network drives, mailboxes) or on external carriers like USB flash drives or CDs/DVDs. Germany was represented by **Olmogo**, a patented mass storage system utilising a client-side encryption for data elements of any size called mogos that can be shared with other users. The users have full review and control over their data. Another participant in the Pitch Deck Contest was **Identt**. This Wroclaw-based, dynamically developing startup offers a wide range of cybersecurity services – from penitentiary tests and security audits to proprietary

Contest winner GREYCORTEX during his speech

and innovative solutions such as idenTT Verification System. It is a tool that helps verify the authenticity of a document by comparing a photograph of the owner with the photograph in the document.

CryptoMind also had a chance to pitch their product, UseCrypt, during the CYBERSEC conference. It is an innovative end-to-end encryption method to store data in the cloud that employs CryptoMind's in-house developed encryption system. UseCrypt is operated via an app installed on a customer's platform, allowing them to connect to the cryptographic data transfer server system. Data is always stored and processed on the server in an encrypted form. Data encryption occurs on a customer's device (smartphone, tablet, laptop), with the use of locally generated symmetric keys. **TypingDNA** is a startup that came to Krakow from Romania. Their develops authentication solutions based on the 'keystroke dynamics-as-a-service' model. The solution is designed to recognise people by the way they type, thus enabling companies and users to verify identity online. This method can be deployed on the existing equipment; it does not require

Bruno Ferreira (left) and Debneel Mukherjee were members of the jury.

special hardware or software downloads – all the user need is a keyboard or a smartphone. **Rublon** is cloud-based software that helps companies protect their users, data and applications, providing trusted access via user-friendly, two-factor authentication. Users confirm their identity by clicking on a link that Rublon sends via email. Then logging from the same device requires only a password. The startup also offers a mobile version of its flagship product.

UNLOQ from Romania also presented an authentication solution using a phone. With identity registration solutions, distributed authentication, different kinds of data encryption, flexible data access rights management, UNILOQ helps standardise and protect stored data. They are securely saved with trusted providers such as Amazon Web Services and Bahnhoff. **Safelly** is a startup from Katowice, Poland. It was founded in response to a dynamic development of the e-commerce market and its influence on Internet marketing, causing a significant increase in cybercrime. Safelly aims to ensure business continuity and liquidity of Internet-based enterprises. The platform operates in a SaaS model and the communication between Safelly and its users is protected with 4096-bit RSA encryption keys generated individually for each site. **Cryptelo** is another Czech startup that we hosted in Krakow. By using the Cryptelo Platform, enterprises that work on sensitive data can enjoy the advantages of easy-to-use cloud or storage and collaboration tools at the company's headquarters, in a completely secure environment. In addition, Cryptelo offers Cryptelo Drive, a solution that makes data impossible to read without the permission of their owners. It protects against industrial espionage, hacking attacks, insider threats and cyberattacks. The service provides secure access to files from any computer, without specialised software. ■

The contest took place at the Innovation Stage of CYBERSEC.


CYBERSEC
EUROPEAN
CYBERSECURITY FORUM
Kraków
8-9.
10.
2018
THE QUEST
FOR CYBER TRUST
STATE
STREAM
DEFENCE
STREAM
FUTURE
STREAM
BUSINESS
STREAM

INTERVIEW WITH DEBNEEL MUKHERJEE

Debneel Mukherjee (center) at the Start-up Pitch Deck Contest, with Ewa Abel (right) and Bruno Ferreira (left).

Robert Siudak: For a few years now, cybersecurity start-ups have been in the spotlight: there has been a growing number of unicorns, more Venture Capital investments, and new acceleration programmes dedicated only to this sector. Many investors believe cyber is the new FinTech. Do you believe so, too? Is this hype and a buzzword or a long-lasting trend?

Debneel Mukherjee: I believe cybersecurity is more disruptive than FinTech. It is not hype but certainly a reality. It has overarching implications on the security profile of our planet: right from simple IoT-enabled home devices all the way to national security and the strategic wellbeing of our civil society.

R.S.: Decacorn Capital, a truly global VC you have founded, has a proven track record of really successful investments: Snapchat, Lyft, Spotify – to name but a few. What is the key differentiator you are looking for in a start-up? Is it region dependent? For example, in search for innovation, do you focus on something different in Europe than in India or the U.S.?

D.M.: We put emphasis on the game changing businesses that are run by outstanding founding teams with grit and ability to execute. While in Europe and the U.S. we look for deep tech innovative game changing ideas, in Asia we look for large untapped opportunities for inclusion of the half the world population that live and play there, most with favourable demographics aspirational value, but low adoption curve.

R.S.: During the European Cybersecurity Forum – CYBERSEC 2017, you were a juror at the Start-up Pitch Deck Contest, watching presentations of 15 young companies from Central and Eastern Europe.

What would be your main piece of advice for them? Where are they lagging behind in comparison to their competitors from the Silicon Valley or Singapore?

D.M.: They must focus on tangible incremental traction that is quantifiable. They need to use speed as capital to build entry barriers and focus on creating delight or solve a true problem, be disruptive and try to avoid crowded space. They must compete with themselves and not with competition. They must be prepared to try and fail, and investors or the ecosystem must not see that as a stigma.

R.S.: How to support young companies with smart not dumb money? What kind of support, apart from investment, should a VC fund offer to their portfolio start-ups?

D.M.: The biggest DO for the VC funds is to help start-ups connect to (a) new markets in order to scale and (b) larger investors for follow-on funding instead of micro managing the founders and telling them how to run their business. The VC fund must not be a control freak and should not try to seek stakes bigger that the founders in the start-ups. Instead, a true VC fund would always try to protect the founder's skin in the game and prevent them from diluting too fast too far, at least in the early years.

R.S.: What are the biggest mistakes start-ups make while raising VC money?

D.M.: Here are a few mistakes to avoid:

1. Look for any money in desperation instead of smart money.
2. Dilute too much too quickly.
3. Raise at valuations that are not defendable later on.
4. Lack of chemistry between the VC fund and the founders
5. Fail to allocate capital frugally. After all, every dollar saved from splashing is every dollar put to build the business. ■

Questions by Robert Siudak

Debneel is the Founder and Managing Partner of Decacorn Capital (Decacorn), a cross border, stage agnostic, venture investing initiative curating best in class businesses from around the world. Decacorn's investments are spread around USA, Europe, Israel and India and has recorded its first stellar exit within a year of its investment.

A chartered accountant by training, Debneel gave up his banking career in 2001 and relocated to Singapore from India to set up a Fintech startup which he successfully exited in 2011.

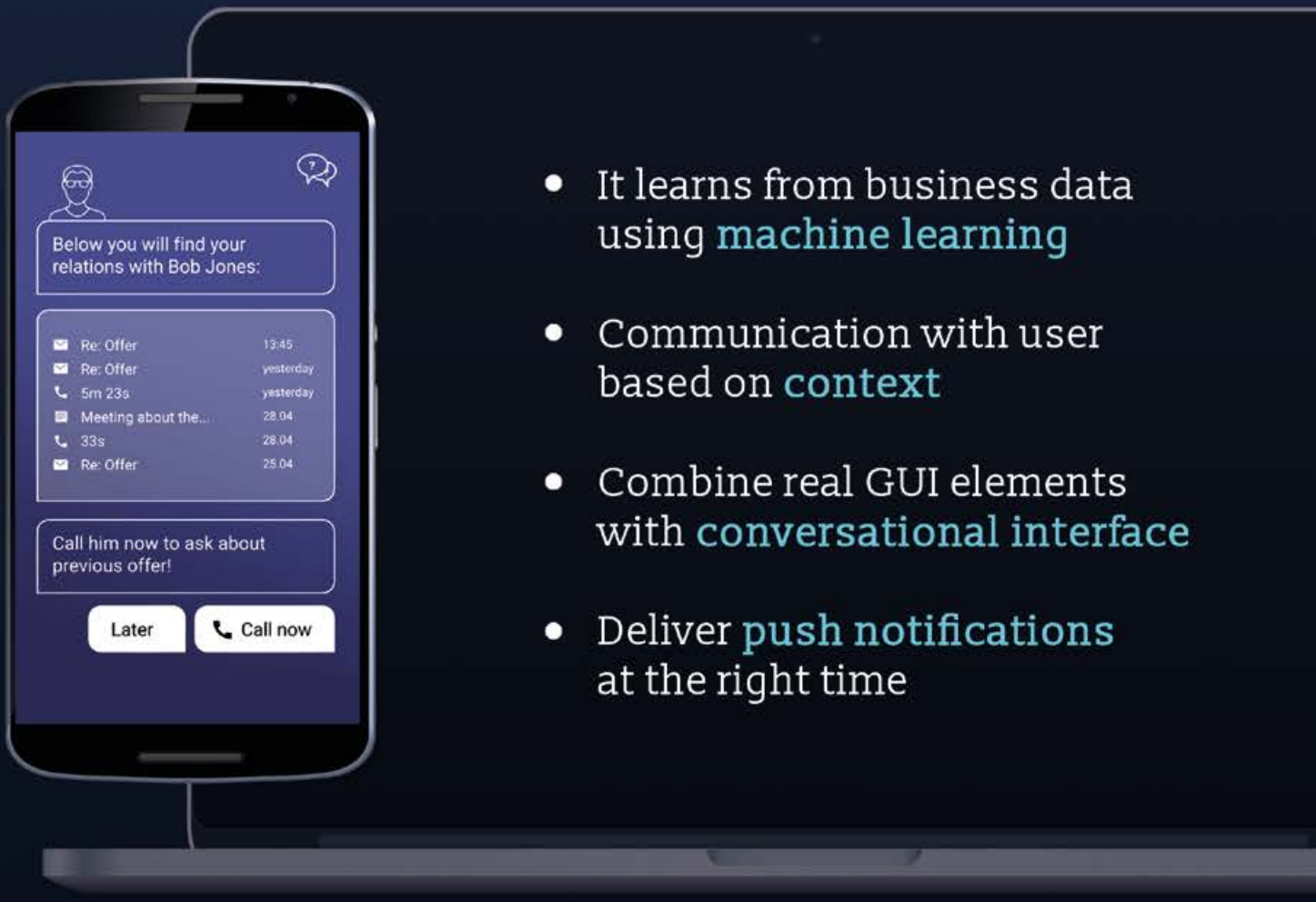
In 2012, Debneel co-founded the seed stage VC accelator WavemakerLabs (WaveMaker) with 6x co-investment mandate from the Singapore Government. Wavemaker made twelve investments between 2012 and 2015, notable among them being Luxola, Tradegecko, Zumata, ArtofClick, and GushCloud.

In 2015, Luxola was acquired by Sephora (a Louis Vuitton Company), and GushCloud by Yello Digital Marketing of Korea. Both deals are counted among the top quartile exits in the Singaporean start-up ecosystem. Later in the year, Debneel sold his entire founding shares in WaveMaker to a Los Angeles based VC fund.

With no inheritance he has created all his wealth from astute investments which he has now put to work in Decacorn. Like him, all his partners in Decacorn are eating their own cooking. As part of his giving back to the society, he is a mentor at The FinLab which is a 50:50 joint venture between Singapore Government (SGInnovate) and UOB Bank Singapore.

Do you know that by 2040 artificial intelligence will be as smart as humans?

Using technology based on deep learning algorithms we are creating a new category of software.

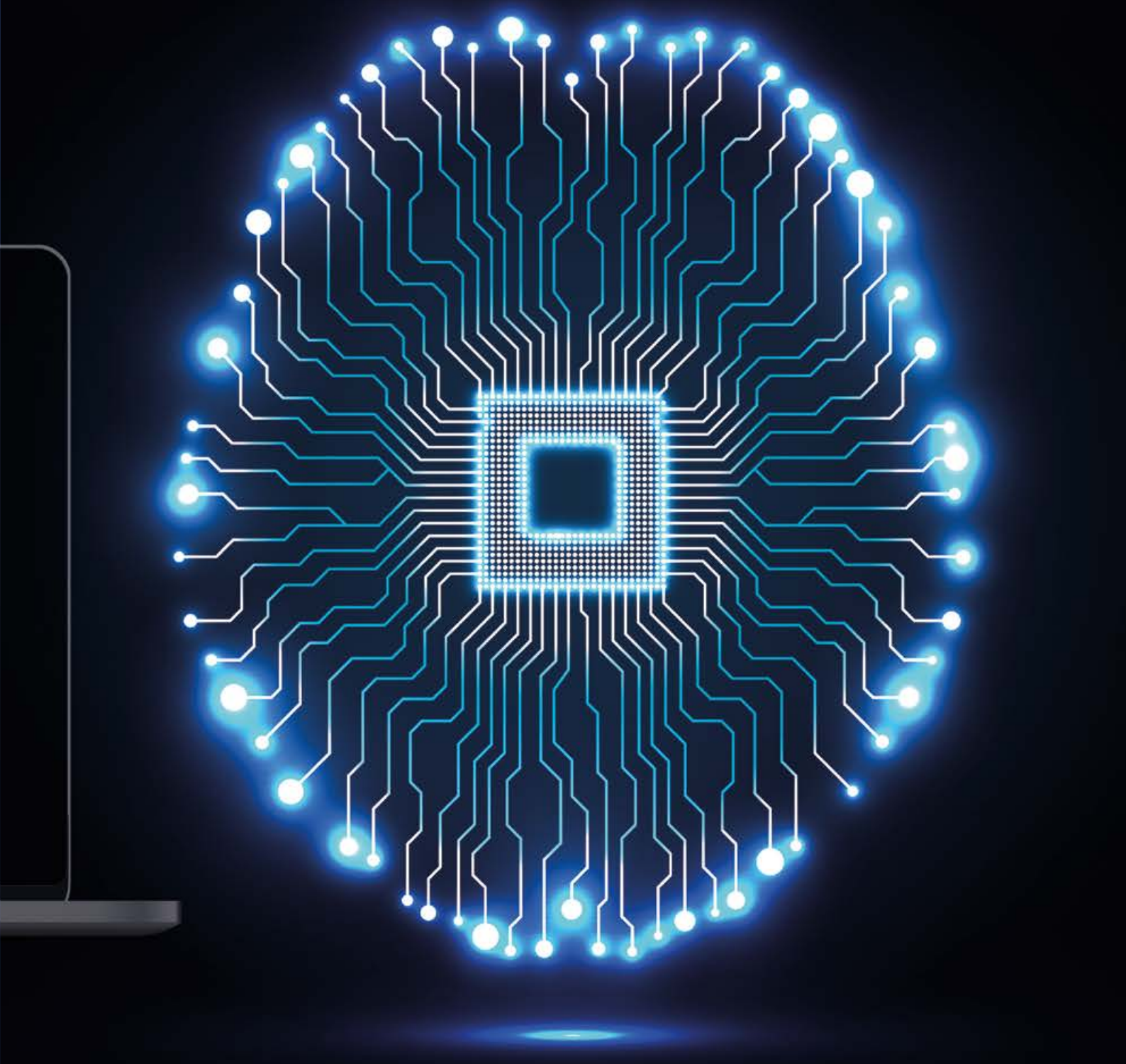


- It learns from business data using **machine learning**
- Communication with user based on **context**
- Combine real GUI elements with **conversational interface**
- Deliver **push notifications** at the right time

2040.io

ul. Podole 60 Krakow, PL
Contact us at info@2040.io

A.I. for your business



www.2040.io

THREAT HUNTING REDUCES DATA BREACH COSTS

BY MARTIN KOREC

On a daily basis, networks worldwide face threats from cyberattacks. These attacks have a variety of sources and consequences, but all present a series of risks to the affected network. These risks are not always the most obvious, or confined in scope.

As networks have grown and threats have advanced, so have security tools, which now include SIEMs, IDS/IPS, sandboxing, etc. Each does a particular job; protecting the perimeter, correlating events within the network, isolating devices, cleaning infections, etc. It is common to both use multiple tools, and to use more tools as its network grows larger. However, each of these tools, because of both their individual natures and the nature of evolving cyberattacks, have gaps in the coverage they provide. These gaps can be exploited by an ever-increasing group of "Advanced Persistent Threats". In fact, according to a Ponemon Institute survey, the average time to detect advanced threats was 49 days in 2016 [1]. Advanced Persistent Threats, or APTs, are:

> *"[a] set of stealthy and continuous hacking processes often orchestrated by human targeting a specific entity. [...] As the name implies, APT consists of three major components/processes: advanced, persistent, and threat. The advanced process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The persistent process suggests that an external command and control is continuously monitoring and extracting data off a specific target. The threat process indicates human involvement in orchestrating the attack"*[2].

[1] Trustwave Holdings, "Trustwave Global Security Report", 2017. [2017-11-30]. http://bit.ly/2mY5JYz.

[2] MUSA, Sam. "Advanced Persistent Threat", 2014. [2017-11-21]. http://bit.ly/2F0FGaT.

Luckily for network security professionals, "Threat Hunting" – or the proactive search for hidden threats – exists as a possible process-based solution. I will discuss this process in greater detail later in the article, including its pros and cons. First, let us present the business risks that these APTs pose.

1. Risk of Data Breach

Almost every cyberthreat has the goal of stealing or modifying company's data. Malware is all over the Internet. Its threat is real and it was cited as the leading cause of attacks leading to data theft in a 2015 report from Kaspersky Labs[3]. In the network setting, it can get into the network via unwary employees, injected to a device by unknown or unpatched vulnerability. Secondly, disgruntled employees may act as threats. The employee is already within an organisation's network, so it is much easier to do damage to data or steal company information.

These two classes of threats can be generally countered in their basic forms by existing security solutions already in place at the customer's network[4]. But this still does not solve the problem of APTs or other threats which can bypass existing security tools.

Financial and Data Loss

Data breaches result in loss. But this loss is not just the "physical" data which disappears or is copied and "lost" in terms of privacy and confidentiality. Data breaches create economic loss. These financial losses include a wide variety of components; from the value of the stolen data, to the cost of technology to remediate it, to the fees for outside personnel like lawyers, PR teams, and risk managers commonly hired to help the company recover[5].

The cost of compromised data varies by industry type and the kind of data stored. The cost of the data breach itself runs in millions of dollars and may vary depending on both the geographical location of the attack and the type of data stolen. For example, according to a recent report by Accenture, the average cost of a cyberattack was USD 11.7 million, an increase of 27.4%, but the cost was higher in the US (USD 21.22 million) and lower in Australia (USD 5.41 million)[6].

There are further costs associated with data breach as well. Not the cost of the breach itself, but the follow-up costs which come from the damage to the business in terms of reputation, stock value, customer loss, etc. Business disruption, including business process failures and lost employee productivity, can be more than half of a business's annual income. Some hackers aim directly for a company's financial accounts instead of customer data, and gain access to its money[7]. In most cases more than half of critical business data is on unprotected devices. Some companies have certain cybersecurity solutions applied in their infrastructure, but mobile devices are often unprotected. The right security solution with full network visibility can help to solve this problem easily[8].

The Hidden Costs

Remediation of the breach can be even more expensive than the breach itself. Breached companies can attract government fines. Customers may sue. But legal and remediation costs are not the only hidden costs. A data breach harms brand and reputation, resulting in the loss of income through sales. Notifying clients of security breaches involving personally identifiable information, which is legally required, can cost a million dollars or more, depending on the size and type of company. Furthermore, not only IT professionals mitigate data breaches. Recovering from a breach is usually done with the help of external experts. PR consultants help with disclosure to the public and clients. Risk management consultants and lawyers help as well. Their cost varies from USD 10,000 to a USD 250,000 per single data breach.

[3] Kaspersky Lab, "Damage Control: The Cost of Security Breaches IT Security Risks Special Report Series". [2017-11-21]. http://bit.ly/2mVxdhJ.

[4] Basu, Eric. "The Top 5 Data Breach Vulnerabilities" Forbes, 2015. [2017-11-21]. http://bit.ly/1HdmhD2

[5] Op. cit. Kaspersky Lab.

[6] Ponemon Institute (jointly developed by Accenture), "2017 Cost of CyberCrime Study. Insights on the Security Investments that Make a Difference", 2017.

[7] Op. cit. Kaspersky Lab.

[8] Sthanu, Subbu. "BYOD 2015: Data Loss, Data Leaks & Data Breaches", DARKreading, 2015. [2017-11-21]. http://ubm.io/20uuvx7.

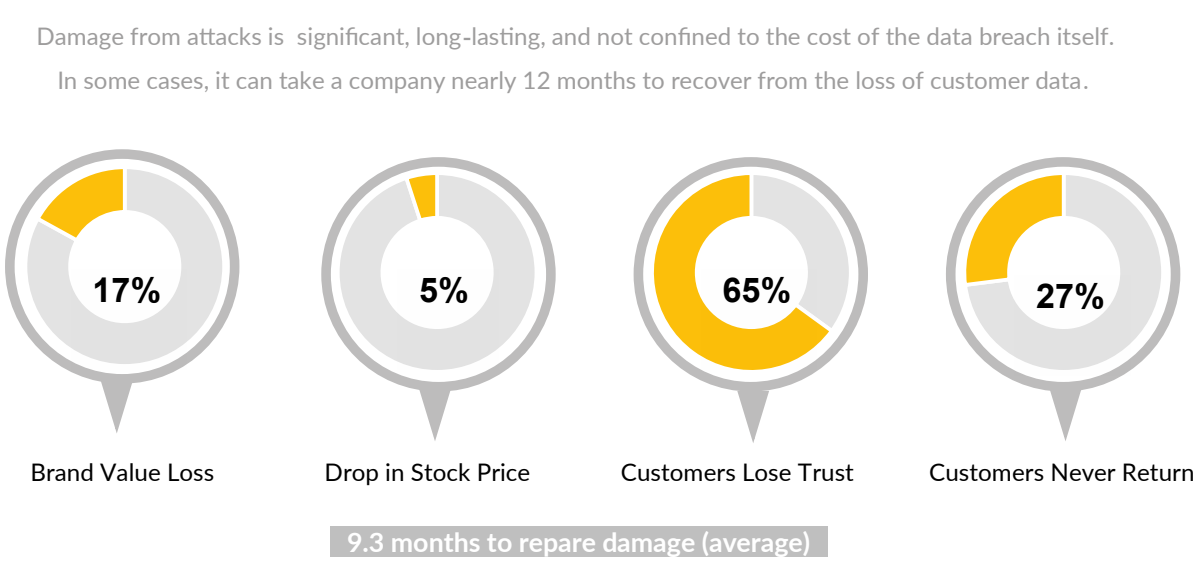


Figure 1. Damage is Real. Source: GREYCORTEX, 2017. Based on Ponemon Institute studies 2011–2017

To fully recover from a data breach can take an unprepared company up to three years[9].

Finally, despite the best efforts of PR consultants, lawyers, and IT staff, "full" business recovery is not guaranteed. Reputation damage—the loss of customer sentiment—may never recover fully and may continue to damage business in the long term. Critical data losses may drive small and medium companies go out of business within a year.

2. Threat Hunting: An Essential Technique for APT Detection

There are many variables that contribute to the total cost of data breach, but one thing is certain: protection, prevention, and detection can greatly reduce risk and cost. As mentioned above, APTs and other attacks enter the network through gaps in existing security tools and may remain hidden for some time. "Threat hunting" or "cyber threat hunting" means proactively and iteratively searching through networks and datasets to detect these threats. It is commonly performed within an organisation by a Threat Hunter and/or Security Analyst. It is an essential process for network security because it works to identify hidden threats within an existing set of network data.

Threat hunting uses manual and machine-assisted techniques, which aim to find Tactics, Techniques, and Procedures (TTPs) of advanced adversaries. While this methodology is both time-tested and effective, it is also time-consuming, and can sometimes miss important clues in the mountains of network data, but it can be made more efficient using more modern tools[10].

Traditional Threat Hunting

Traditional threat hunting is done as early-stage threat detection. Here, the focus is on identifying threats as early as possible with the help of tools that gather data and export them usually to an SIEM system. It is not very effective, and mostly involves an analyst looking for threats manually in SIEM exports, or looking for infection on devices. Traditional threat hunting is more based on human capabilities and experiences rather than relying on analysis security tools. This approach is common, because it is easy, and most organisations are satisfied with their threat-hunting programs. Previously undetected threats are found via basic threat hunting, but this still only scratches the surface. Anomalies, user actions, and advanced threats remain undetected when relying only on traditional/basic threat hunting. More than half of companies

[9] Filkins, Barbara. "Cleaning Up After a Breach Post-Breach Impact" SANS Institute, 2015. [2017-11-21]. http://bit.ly/2Dmo091.

10 Lee, Robert M, Bianco, David. "Generating Hypotheses for Successful Threat Hunting", SANS Institute, 2016. [2017-11-21]. http://bit.ly/2Dw70jV.

still do not have a threat-hunting program in use, and those that have threat-hunting programs are using those that are mostly ineffective and outdated. Using an advanced security tool and a right cyber threat-hunting methodology makes a significant difference in the early detection and elimination of threats[11].

A good threat-hunting tool supports the analyst by providing ready access to data in the analysed network. As techniques have evolved, the idea of the "Intelligence-Driven Hypotheses" has gained popularity. This concept includes awareness of threat intelligence, the use of Indicators of Compromise (IOCs),

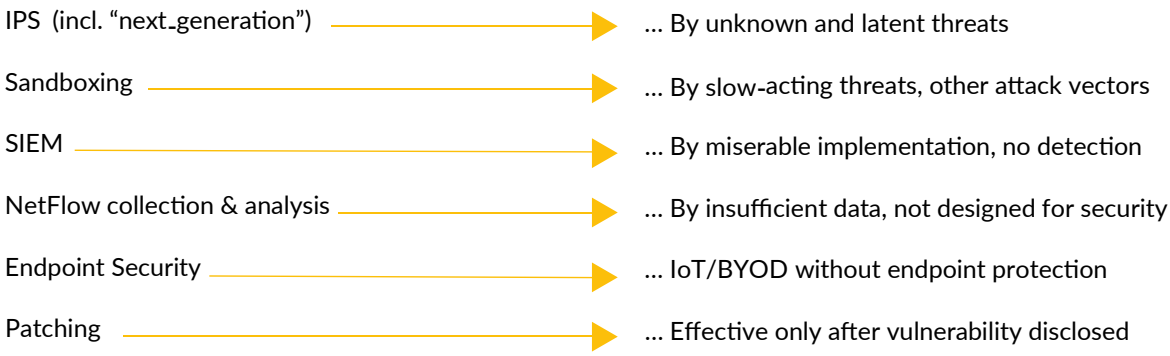


Figure 2. Advanced Threats Prey on Weaknesses in Existing Tools. Source: GreyCortex compilation based on various studies[12]

3. Modern Cyber Threat Hunting Methodology

Threat hunting is an iterative process that repeats a series of steps to continuously look for adversaries hidden in vast datasets. The steps are: hypothesis creation, hypothesis testing, investigation of old data and discovery of new threats, and finally informing analytical models. These steps can take a significant amount of time if done by traditional means; modern techniques and tools can help shorten the process considerably.

The first step is to create a hypothesis. The hunter needs two key components: the first is an observation of possible threats or events. The second component is that the hypothesis must be testable. To fully test the hypothesis, the hunter requires the right analysis tools.

with existing TTPs. Hunters must note where IOCs or events come from in terms of phases of the kill chain. But if a hunter tries to generate a hypothesis that demands an analysis of all data from every IOC, it may be overloaded with low-quality information. Instead, when the hunter uses the right IOCs—as provided by tools with correlation, full network visibility, and machine learning—this will help shorten the time needed to understand adversary TTPs[13]. Hunters must be careful not to spend too much time on hypothesis generation, which limits the time and opportunity to begin investigating.

Investigation via tools and techniques follows hypothesis resolution. Hypotheses are most effectively investigated via tools and techniques; tools which must be capable of Linked Data Analysis, full network visualisation, correlation techniques, and machine learning.

Uncovering new adversary patterns and TTPs is a very important part of the third step in threat hunting methodology. While it may be done without an automated detection system, detecting new TTPs by traditional methods is inaccurate and time consuming. Having a tool which correlates a series of disparate events and data sets into one actionable threat alert is critical.

[11] Lee, Robert M, Bianco, David. "Generating Hypotheses for Successful Threat Hunting", SANS Institute, 2016. [2017-11-21]. http://bit.ly/2Dw70jV.

[12] Ierace, Nick, Urrutia, Cesar, Bassett, Richard. "Intrusion Prevention Systems", Ubiquity, 2005. http://eues.io/mTS4 Stamp, Paul. "The difference between Endpoint Detection and Response, Sandbox and Containerization Solutions", Cybereason, 2016. http://bit.ly/2DupEcZ ; Keragala, Dilshan. "Detecting Malware and Sandbox Evasion Techniques", SANS Institute, 2016. http://bit.ly/2uSHTkk ; Siakos, Chris. "9 limitations to be aware of when considering Netflow for visibility", Sinefa, 2015. http://bit.ly/2BisU57 ; Wilkins, Sean. "A Guide to Choosing and Endpoint Protection Solution", Tom's IT PRO, 2014. http://bit.ly/2rutLA8 ; Monahan, David. "The Truth Behind the Scope of the Endpoint Problem in the Enterprise", ForeScout, 2016. http://bit.ly/2mZ2Szn ; Lawton, Stephen. "Guide to Security Information and Event Management", Tom's IT PRO, 2015. http://bit.ly/1QrpdyN ; [last access on 2017-11-21].

[13] Op. cit. Lee and Bianco, 2016.

The last step in the cyber threat hunting methodology's iterative process is informing and enriching automated analytics. Having a tool which incorporates machine learning and artificial intelligence is significant in this area, because it essentially saves the step of teaching the threat hunting model new information, because that information is learned independently[14].

APTs Can Be Beaten

Threat hunting is important, but it can be overcome by advanced adversaries. The effectiveness of this process can be improved by using the right tools, which are capable of correlating gathered information, as well as offering full network visibility and machine learning. Second, time is one of the most important metrics in the process of threat hunting. Late threat detection and incident response often lead to successful attacks, which leads to damage, theft, or disruption of a company's information or business. Tools which link a complete set of network traffic metadata in one place (e.g. a single GUI) save valuable time, both in threat hunting and in detection overall[15].

4. Use Cases

While it is possible to discuss threat hunting in abstract terms, use cases give a more complete understanding of the process and of how the right analysis tool makes threat hunting easier. Below are three of the best-known types of advanced TPPs.

Uncategorised Proxy Events

Some adversaries use uncategorised domains for attacks, because simple rule-based detection mechanisms do not trigger them. Detecting the source information of possible attacks is difficult with most network security tools, which lack proxy visibility. Traditional proxy servers create a gap between associating security events and network traffic with a proxy address and the actual address of the domain used by the adversary. Some security analysis tools provide proxy visibility, which closes that gap and associates network flows behind a proxy with network flows inside the local network to create a single network flow, visualised with details about the communication. This additional visibility allows the threat hunter to detect and respond to threats in a matter of minutes[16].

Command & Control

Adversaries can establish command and control over devices with a variety of covers, depending on network and system configuration. They can define new protocols and use existing, legitimate protocols and network services for communication to evade firewall and security policies. Detecting command and control activity in network traffic can be tricky, and most tools rely on signatures for unique indicators within protocols. However, an adversary can construct their own communication protocol in such a way that it avoids detection. Prediction Analysis, based on supervised learning, can detect anomalies in port entropy, service usage, and botnet communication. Another helpful component of analysis tools with command and control detection capabilities is Repetitive Analysis, which recognises periodic behavior patterns and machine communication of advanced malware and users. Using these tools, an analyst can discover command and control attacks[17].

PowerShell Misbehavior

Attackers do not always create their own tools for attacks. Increasingly, they are leveraging tools that are already present on the targeted device. One of the most commonly used is Microsoft PowerShell, because it is installed on every Windows system by default, and is not as suspicious as external tools used for attacks. The majority of enterprises use Microsoft Windows on their computers and devices. It is used by administrators daily, so scripts used by adversaries are easily obfuscated. PowerShell scripts can be present as external files or Microsoft Office macros, which is why such malicious scripts cannot be reliably detected by tools using static signatures and similar techniques.

[14] LEE, Robert M, LEE, Rob. "The Who, What, Where, When, Why and How of Effective Threat Hunting", SANS Institute, 2016. http://bit.ly/1sP9nF7.

[15] Op. cit. Cole, 2016.

[16] Sanders, Chris. "Threat Hunting for Uncategorized Proxy Events", SQRRL, 2017. [2017-11-21] http://bit.ly/2DsAe46.

[17] Definition of "Command and Control", MPN platform. [2017-11-21]. http://bit.ly/2G3tdEr.

Detection of attacks like these can be done by advanced signature-based analysis and machine learning detection engines[18].

Conclusion

Cyberthreats, data breaches, and data losses create a variety of risks for the company that suffers them. The unifying theme is that these risks/results all cost a lot of money to repair. But while these costs may be predictable in some ways (e.g. the cost to remediate a data breach or the value of the lost data itself), hidden costs, like damage to business reputation, sales, stock price, customer sentiment, etc., as well as the cost to hire auxiliary staff to resolve these hidden risks, can have additional and significant costs, which may be greater than the cost of the data itself and may be something from which the business is never able to recover.

Threat hunting is an important means of detecting these threats before they can cause a data breach. Traditional threat hunting can become bogged down by massive volumes of data and take time, which leads to late threat discovery. Luckily, modern security tools not only help speed up the detection process by triaging, correlating, and providing full visibility into possible IOCs, but are also able to learn and analyse network traffic independently for more effective detection. ■

ABOUT THE AUTHOR:

Martin Korec is Chief Product Officer at GREYCORTEX. Martin currently oversees the product vision of the MENDEL network traffic analysis solution, as well as teams engaged in its research and development. In addition to a strong personal and professional interest in cybersecurity, Martin has studied cybersecurity at the Faculty of Informatics at Masaryk University. In his spare time, he writes and publishes articles for security magazines.

[18] Symantec, "The Increased Use of Powershell in Attacks", 2016. [2017-11-21] http://symc.ly/2hmAQMh.

THE FRENCH CYBER SECURITY MARKET

BY AMÉLIE RIVES

Under the combined impact of digital transformation and the advent of new technologies, challenges related to identity and data protection, the emergence of new cyber threats, and a surge in cybercrime, cybersecurity has become a priority for French government and businesses. It is now definitely a competitiveness opportunity and an area of growth.

In the meantime, several cases of espionage and state sponsored cyberattacks have made the cyberspace a new strategic space likely to bring about new opportunities for the French industry. In this context, it is worth analysing how the French market compares to world and European markets in terms of size and development, but also what its specificities and vulnerabilities are and how these could impact future developments. Initiatives and efforts taken to mitigate potential adverse effects are also interesting to look into, particularly those aimed at strengthening the cybersecurity industry and at better structuring the national cybersecurity sector.

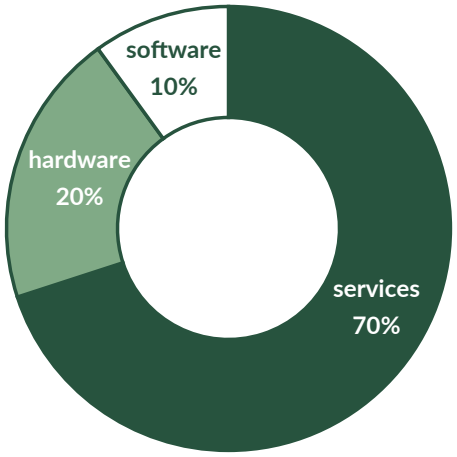


Figure 1. World ICT market: repartition of revenue. Source: Gartner, 2015[1]

A Dynamic and Fast Growing Market

When compared to world and European markets, France appears to be quite well-positioned and to feature similar trends and tendencies in terms of growth and progression.

According to a study by Gartner[1], the world ICT market reached €3.2 billion in 2015 and is expected to reach €3.4 billion in 2020. 70% of this total revenue should flow from services, 20% from hardware and 10% from software. The same Gartner report shows that world market for cybersecurity grew from €3.1 billion in 2004 to €67 billion in 2015, and should reach €152 billion by 2020. I n the same period, the value of the ICT market in France approached €105 billion in 2014 after a 10% increase, and the cybersecurity market reached €1.8 billion in 2015 versus €1.6 billion in 2014, that is a 12.5% increase[2]. While these figures show that France follows the global trend towards a further and faster digitalisation and cybersecurity, a closer look at the ICT/Cybersecurity ratio tends to suggest, however, that it is a little behind world and European cybersecurity markets: in 2014, cybersecurity only represented 1.7% of the French ICT sector, when the world ratio was at 2,4%[3]. But in the context of a continuous and ever faster growth of cybersecurity in both world and French markets, it is fairly reasonable to expect this gap to be filled very quickly, with France quickly catching up with global markets.

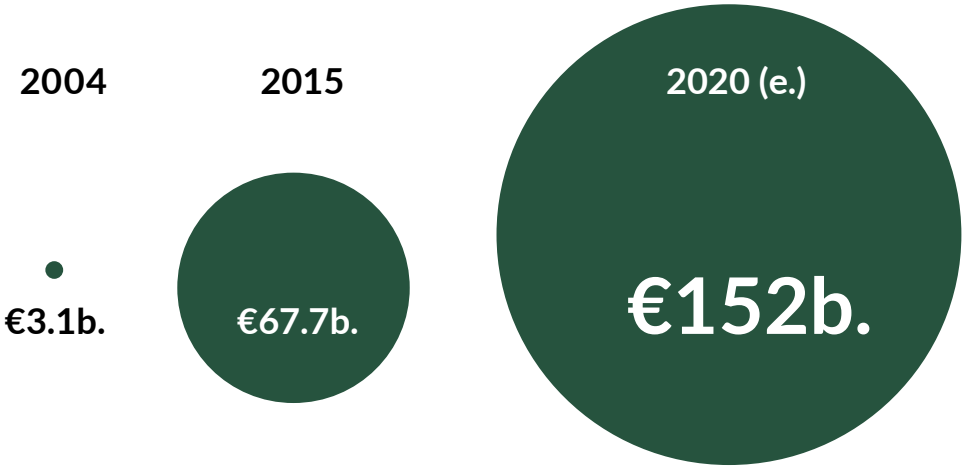
In fact, cybersecurity remains a very dynamic sector in France, as exemplified by its frequent and rapid developments (acquisitions, investments, significant increases in turnover, diversification…). Driven by a growing public procurement and new national and European regulations, cybersecurity has become a priority for many companies across industrial sectors. For instance, the new Military Planning Law includes a cybersecurity section that requires critical national infrastructure operators to implement a series of protection and detection measures and processes.

[1] "Forecast Analysis: Information Security, Worldwide, 2Q15 Update.", Gartner, 2015.

[2] *"Le marché français de la cybersécurité en France et dans le monde"*, Xerfi, 2015.

[3] *Ibidem.*

Figure 2. Estimate value of the world ICT market. Source: Gartner, 2015[1]



This is expected to bring about a significant increase in these companies' security spending and budgets in the coming years. The European Network and Information Security Directive—which aims at aligning Member States' obligations in terms of information systems protection–should also boost the French cybersecurity market.

But while the French market is undeniably following the same path as global and European markets in terms of growth and progression, it also features structural specificities that could impact future developments and that are likely bring about internal changes.

The new Military Planning Law includes a cybersecurity section that requires critical national infrastructure operators to implement a series of protection and detection measures and processes.

A Diverse But Fragmented Sector

The French cybersecurity market is unquestionably diverse, encompassing the vast majority of cybersecurity products, solutions, and activities across industry segments and business lines. Software and hardware offers include surveillance and perimeter protection, advanced threat and vulnerability detection and analysis tools, encryption tools, secure identification and authentication tools, and specialist tools (forensics, integrity checks, surveillance…). As for services, they range from audit, consulting, and governance, to integration and externalisation. Other prominent areas are web hosting and cloud services offers, featuring a mix of hardware, software, and services.

These industry segments and business lines are of course not equally represented among the sector's players. This is mostly due to the structure of the French market, which is extremely fragmented. It is generally agreed that about 450 organisations operate in this sector, either companies exclusively offering cybersecurity products/services, or companies that include cybersecurity offers among a wider range of products, solutions or services. After a more detailed analysis of these 450 companies we chose to only consider 250, excluding local branches of foreign companies, recent acquisitions, and buyouts. These 250 companies generated a total turnover of about €2 billion in 2015[4].

A key element to understand the structure of the market is the fact that just 26% of these (25 companies) generate 75% of the total market turnover (€1.5 billion annually). Even more telling is the fact that only 30 of the remaining 225 SME exceeded €5 million of annual turnover for a total of €416 million in 2015, that is 71% of the total annual turnover for the sector[5].

[4] Facts and Figures compiled by CEIS through internal market research and industry interviews.

[5] PIPAME, "Analyse du marché et des acteurs de la filière industrielle française de sécurité – Synthèse", November 2015.

This is a meaningful illustration of the polarisation of the French market, which relies on a handful of big players on the one hand and a galaxy of small to very small companies on the other, with only a few medium-sized companies.

Interestingly enough, none of the key players of the French cybersecurity sector are exclusively cybersecurity companies. Large players, like Atos, Orange, Thales, or Airbus, come from a variety of sectors: defence, specialised consulting firms, telecommunications operators, digital security, etc. All have developed and included cybersecurity offers among an existing range of offers and products but only a small proportion on their turnover is generated by their cybersecurity activities. In other words, the French cybersecurity market is dominated by non-cybersecurity players, subsidiaries or branches of large groups operating in very different–yet not unrelated–sectors and business lines.

The French market [...] relies on a handful of big players on the one hand and a galaxy of small to very small companies on the other hand.

Like their counterparts on global markets, the sector's larger players' offers mainly consist in end-to-end services and solutions combining the implementation of networks monitoring and protection strategies, steering and governance solutions, and Identity Access Management related services. The prominence of services is also reflected at the SME level, where they clearly prevail over software and hardware solutions with respectively 46%, 39% and 9% of the sector's 225 SME's annual turnover[6]. SMEs operate mainly in three subsectors: Training, Consulting and Services (30% of the market's players, 46% of the market's annual turnover in 2015), encryption, signature and authentication tools (29% of the market's players, 11% of the market's 2015 turnover), and analysis, detection and mapping tools (23% of the market's players, 17% of the market's 2015 turnover).

These 3 subsectors enerated €453 million in 2015[7]. Only far beyond are segments like hardware, CMS tools and infrastructure operators, and OS/proactive combat tools.

Towards a Structured and Concentrated French Cybersecurity Industry?

A lot of work and efforts have been done to better understand the causes of this situation, to raise awareness among public and private decision makers, and to recommend actions and solutions to initiate a structuration and an upscaling of the French cybersecurity industry.

The PIPAME study lists the structural, behavioural, and policy weaknesses that hinder the development of a strong and structured cybersecurity industry. In addition to those listed above, structural factors include a lack of skills and inadequate training programmes, and the absence of shared practices (norms, processes and standards) and certification processes at the European level. Behavioural weaknesses range from a lack of confidence and ambition from SMEs themselves, to a certain unwillingness from major contractors to allocate enough resources to security and to innovate in this area, and to insufficient strategic and operational efforts to avoid national champions from being bought-up. The lack of private investment represents another serious obstacle: private investors participate in the capital of less than 20% of the companies considered in the PIPAME reports, while external investment only amounts to an average of €3.1 million per company[8]. Public investment remains equally limited, and the French sector suffers from a glaring lack of schemes and mechanisms aimed at supporting support innovation on one hand, and substantial state subventions on the other.

It can be inferred from the nature of the abovementioned factors that these structural and behavioural weaknesses can only be overcome if government agencies and private actors join forces to design and implement national strategies and dedicated public policies.

[6] Facts and Figures compiled by CEIS through internal market research and industry interviews.

[7] www.entreprises.gouv.fr/files/files/directions_services/etudes-et-statistiques/prospective/Industrie/2015-11-Filiere-securite-pipame.pdf

[8] Op. cit. PIPAME, 2015.

What is required is a top-down process launched jointly by industry and government decision makers and embodied in a strong and proactive industrial policy aimed at upskilling national cybersecurity players and at scaling-up the cybersecurity market. The latter will have to include at least (but not exclusively): R&D, normalisation and certification, and export support.

In this respect, the role of the ANSSI[9], the National authority in the area of cyberdefence and network and information security, is instrumental. As part of its three core missions to prevent, defend, and inform, the ANSSI is "responsible for creating the conditions for an environment of trust and security favourable to the development of the information society"[10]. The agency comes in as a key element in the promotion of national know-how, systems, and technologies, and it contributes to the protection and defence of the economic potential of the nation. In fact, the ANSSI plays a leading part in the development of a high-grade national product and service offer through different means, ranging from product and services specification to issuing licenses and qualifications certifying that cybersecurity products comply with set technical specifications. By providing information and advice, and by playing a consulting and support role for government and critical infrastructure operators, the ANSSI also helps local actors to better adapt their knowledge of and capacity to respond to cyber threats, thereby further upgrading the national services and products offer. It also does so through continued efforts and initiatives aimed at steering French and European research.

ANSSI plays a leading part in the development of a high-grade national product and service offer through different means.

Encouraged and facilitated by the ANSSI and other relevant government departments and industry players, initiatives aimed at addressing these shortcomings are mushrooming. Concrete projects benefiting from government backing, support, and in some cases even funding, have already been set-up, and ad-hoc working groups have also started to write roadmaps in a variety of areas. Such was the objective of the Cybersecurity working group set up by Allistene, a public research body, or the "Cybersecurity plan" designed by the ANSSI as part of the Ministry of Economy "Nouvelle France Industrielle" (New Industrial France") project. Other initiatives include the "France Cybersecurity" label or the Cybersecurity Observatory, among many others[11]. Clustering tech startups, research centres, and entities working in the field of cybersecurity is also a first important step towards a better structuration of the French industry. There were 7 clusters totalling 263 members with activities related to cybersecurity in 2014, either as their exclusive activity, or as part of a wider range of activities[12].

Conclusion

Much still remains to be done but the seeds have been sown, the foundations have been laid, and the reasons to be optimistic are many. Boosted by willing decision makers, proactive local authorities, and industry groupings, and driven by a seemingly unstoppable digital transformation, chances are high that the French cybersecurity market will quickly overcome the existing vulnerabilities to better exploit its assets and to unlock its potential. Challenges ahead include fostering further cooperation, better coordination and more synergies between public and private actors, Defence players and critical infrastructure operators; the establishment of a clear and assertive industrial policy aimed at enhancing the visibility of the sector's startups both locally and on international markets, at setting up export support schemes and innovation support mechanisms, at boosting R&D; and at reinforcing collaboration and harmonisation at the European level to approach international markets from a stronger position. ■

[9] Agence Nationale de la Sécurité des Systèmes d'Information.

[10] www.ssi.gouv.fr/en/mission/audiences-and-activities/

[11] Systematic Paris-Region and Hexatrust, "Cybersécurité & Confiance numérique", 2017.

[12] Op. cit. PIPAME, 2015.

ABOUT THE AUTHOR:

Amélie Rives is a senior cyber security consultant at CEIS, a French strategic consulting firm with a focus on defence and security. Amélie mainly works on cyber security and digital transformation for clients such as the French Ministry of Defence. She is also the programme manager for the International Cybersecurity Forum (FIC), an international annual event organised jointly with the French Gendarmerie Nationale.

Sher.ly is a SaaS data smart syncing & collaboration service for business. It delivers a new way of sharing your sensitive files with your co-workers and business partners by creating a secure, invite-only network on demand. It works like a cloud, but all the data stays on your own storage.

ABOUT SHER.LY

Sher.ly is a startup launched in 2013 dedicated to creating innovative software for file sharing among business organisations, on both desktop and mobile devices. The main development centre is based in Krakow, Poland. The company gained traction in June 2014, mainly thanks to a crowdfunding campaign on Kickstarter. The financial target was met in 223% and Sherlybox became a huge success even before hitting the market in August 2015.

We offer you the Sher.ly application, for secure and fast data sharing, as well as the Sherlybox device - the embodiment of a private and secure storage cloud for your files, available 24/7.

HOW THE IDEA WAS BORN?

It all started with two friends who were passionate about new technology – Blazej Marciniak and Marek Ciesla. They met and worked together at Veracomp in Krakow, one of the biggest IT distributors in Poland. Before Sher.ly, they created new technology for safe data transmission over the Internet, called VPN. In further development, the idea has been extended by observing users' behaviour, especially related to storing and downloading files from the Internet.

SHARE & SYNS FILES SECURELY DIRECTLY FROM YOUR DEVICE

Sher.ly delivers a new way of sharing files with your co-workers and business partners, directly from your computer or other devices, by creating a secure, invite-only network on demand.

Sher.ly is a perfect and fully secure alternative to public cloud solutions like Dropbox, OneDrive, Box, Apple Cloud Drive or Google Drive because the data is not uploaded to any external servers. With Sher.ly, you create your own virtual drive, an unlimited cloud using the hard drives in your devices. For this reason, you don't pay for any storage capacity in the cloud.

The application uses the latest secure encryption protocols for file transfer and allows you to track the full history of sharing files with individual users. With this solution, the owner of the file has full control of data confidentiality and can control the identity of the recipients right away.

The files are immediately visible in your Sher.ly app thanks to intelligent metadata synchronisation, which allows you to set preferences for sync and access depending on project you've created, device you've used, file name, file size, modification date or sharing party. There are no bulk uploads and downloads, no data size limits.

When a user device goes offline, e.g. a laptop sleeping to conserve power, it's vital for data availability to have always-on networked storage with Sher.ly software on it. You need a physical storage device to keep your data. That is why we invented the Sherlybox storage device.

SHERLYBOX, YOUR PERSONAL CLOUD,
DESIGNED AND BUILDT FOR SHARING FILES

This unique storage device, powered by Sher.ly software, gives you freedom to share files even when your computer is offline. Sherlybox embodies the vision of your own secure cloud for files, available 24 hours a day.

Anyone can install and instantly use Sherlybox. With just a touch of a finger, pairing is done with any device, and three seconds later, you receive secure, unlimited access via Sher.ly app and start a whole new experience of collaboration. Sherlybox is fully compatible with Sher.ly app which mediates and establishes network connections and allows you to work from outside the office in the same secure way like from inside. The data is fully protected, only accessible to authorised users, thereby limiting the data leak risk factor to virtually zero.

Storing data is not enough, Sherlybox's main functionality is to share it, yet separating the data access from device access.

UPGRADE YOUR BUSINESS COLLABORATION TO THE NEXT LEVEL

Sherlybox and Sher.ly Software give organisations the freedom to share any file, with anyone, anytime. Each organisation, each department, each team now has complete control over who, when, and how sharing is done. Sher.ly removes the boundaries of team collaboration.

We are moving far beyond simple file sharing. Our main goal is to create a complete management platform for sensitive data being shared in business, which will facilitate secure & smart workflow across internal teams and external clients.

hello@sher.ly | @sherlyfiles | www.sher.ly | www.sherlybox.com

GDPR IN THE WORLD OF MICROSERVICES

BY ALEKSANDER P. CZARNOWSKI

Two important changes are facing every organisation that employs IT for business purposes: the GDPR compliance and microservices (also known as "microservice architecture"). While the GDPR is a legislative requirement, microservices are only a recent technological trend – one that will eventually be reverted or somehow evolve into something else. The driving force behind the GDPR is obvious: the enforcement of proper handling of privacy data by all entities in the EU (or the processing of the EU citizens' data). We may like or not the conclusion that comes from the GDPR that the only way to achieve this target is to introduce high financial penalties for non-compliance. However, it is impossible to deny the fact that it is fines that have brought everyone's attention to the matter of protecting private data, also called personally identifiable information (PII) or sensitive personal information (SPI).

On the other hand, every developer nowadays seems to be in love with microservices, especially those based on the REST protocol. Microservices allow quicker and easier deployment; thanks to available frameworks and libraries, they are also quick in development, and in the case of the REST-based microservices, they also scale quite well. However, this comes at a price: architectures can become quickly quite complex, meaning that both management and auditing becomes an intricate issue as well.

Advantages of Microservices from the GDPR Perspective

The good news is that some microservice characteristics can be turned into GDPR compliance advantage.

First of all, due to their nature, we have a clear separation of duties and compartmentalisation. Both attributes are crucial to the GDPR's "privacy by design, privacy by default" requirement.

First, in case of a security breach, both mechanisms limit the incident scope. In case of a data leak or other form of unauthorized access, a vulnerability in one of microservices does not lead to automatic penetration of other microservices. In many cases, there is "no reflection" or "transition" of a vulnerability from one microservice to another (although it is technically possible if the same technological stack has been used and both microservices share the same code base). This is quite different comparing to a set of Virtual Machines (VMs) that are created from the same source and may all share exactly the same set of vulnerabilities if not managed correctly.

Second, microservice architecture means limiting functionality of every microservice in comparison to large, monolithic applications that encapsulate their whole functionality into a single application. This has an important security advantage: a single microservice has a much smaller attack surface than a complex application. This means that the vulnerability risk is lower in case of a well-defined, simple microservice. This also means that – at least in theory – an application based on microservices could be more secure by design than a monolithic app.

Containerisation

In many cases microservices are run and managed inside containers. Containers enable quick and easy microservice deployment. From a security and compliance perspective, however, they also bring some issues to the equation:

- Containers are often treated as closed black boxes that do not need management; however, the same security rules like patch management must apply to containers, just like they do to VMs or operating systems running on physical hardware.
- Containers need to be secure, which means that the same hardening rules should apply to them as is the case for VMs or operating systems running on physical hardware.
- Software enabling containerisation like Docker has its own attack surface that needs to be secured before deployment in a production environment.

Since microservices are usually run in a set of containers (less often in a single container), whereby one container provides a web server, another database, and a third one a logging functionality, we can use their container definition files (like docker-compose.yml in the case of Docker for example) to get a description of services. This, in turn, allows us to quickly create GDPR required mapping of data processing processes.

Microservices – Minimal GDPR Requirements

Just like any other software processing PII, microservices need to meet GDPR requirements. Here is a minimal list of safeguards every microservice must provide:

- *Strong authentication* – access to PII must be controlled and strong; sometimes even multi-factor authentication must be in place
- *Strong encryption* – encrypt using approved encryption algorithms for data that is sent over network channels and that is stored in databases and files
- *Access logging* – audit trails for accessing PII must be provided; keep in mind, however, that logs must not contain PII data
- *Only secure component usage* – vulnerable, outdated components must not be used to build a microservice

Auditing Microservices for GDPR Compliance

It is not possible to provide a complete, one-size-fits-all checklist for auditing microservices for GDPR compliance, but the list below is a good starting point:

- Overall architecture – review overall architecture and assure that it can be GDPR compliant, remembering about the "privacy by design and by default" requirement
- Security management – ensure that proper security management like patch management, vulnerability management, or incident management are in place
- Configuration – ensure that production configuration enforces strong security including sessions management, strong encryption; neither passwords nor PII are kept in open form
- Encryption – ensure that proper, strong encryption is enabled for both network communication and data encryption (for example processed in databases)
- Test and Production environments separation – ensure that both environments are separated and there is not direct access from one to the other. Ensure that test data does not contain PII.

Conclusion

Microservices are an important part of current DevOps movement, and unlike GDPR requirements, they will not go away any time soon. Being aware of advantages and security limitations of microservices is a first step to ensuring GDPR compliance for such architectures. However, the increase of architecture complexity may be an important drawback both to compliance and security management. One solution to deal with this problem is to introduce a Secure Development Lifecycle process. The SDL will enable proper design and management of both the developed software and the production environment, making GDPR compliance a lot easier to achieve and manage. ■

ABOUT THE AUTHOR:

Aleksander P. Czarnowski, CEO of AVET Information and Network Security Sp.z o.o, member of the Polish Committee for Standardization (PKN) TC 182 – Information Technology – Security Techniques, responsible for ISO 27000 standards family. Member of Cloud Select Industry Group at the European Commission, member of Advisory Board of the STAR Audit organisation and member of Program Committee of Quality Certification Center at the Military University of Technology in Warsaw.

exit
experts in information technology

INFORMATION IS IN THE CENTER OF EVERYTHING WE DO.

STORE

Are you aware of the place where your information starts and transforms? Is it in your private or public Cloud, or maybe it is in your employees' mobile devices? Do you control how your data is stored and managed?

First thing about the digital information is the place where it lives. Providing safe and effective space, and tools for managing growing volumes of data is essential when thinking about security.

How can we help?

We plan, design and implement advanced architectures for storing and processing data. We think about information as the process that needs to be protected and managed.

BACKUP

Next step in protecting your data is making a copy but in fact the most important thing in backup and archiving data is restoring it. What is more, effectiveness and ease of use should be the „must have" feature of backup solution. If you look forward backup as a service seems to be the most optimal way to provide effective protection for your data.

Do you have a backup policy? Do you test and verify your backup regularly? Do you spend hours and days on managing and enhancing backup solutions?

We can help you by:

- providing advanced consultancy services helping customer to implement best backup and archiving plans and politics,
- taking care of existing backup environments by enhancing and modernizing backup,
- providing BaaS (backup as a service).

BUSINESS CONTITUITY

When your important information in unavailable your business looses. The consequences may be diverse from company image deprivation, through operational outage, financial loss up to total disaster.

Imagine the possibility to work constantly, recover in fast, simple way to the picked point in time despite of the disaster range.

We think about disaster recovery plan as the insurance for your information. We can help you design a high availability solution that best fits your needs and value of your data. Depending on your company's profile we can implement DR on premise, in a Cloud, or as a Service.

SECURITY

Today's threats forces organizations to protect data in the diverse way. You need to manage and monitor your data from the beginning, defining and controlling the access outside and inside the organization, protecting your data from accidental as well as intentional danger.

Our advanced consultancy services can help you to point the most vulnerable areas and to design the consistent policy in area of data security.

EDUCATION

Continuous learning is the best way to stay up to date with dynamic technology growth as well as threats expansion.

We provide broad portfolio of authorial courses that helps IT Professional to develop their knowledge and competences.

It is obvious that you care about your information.
The case is how you provide this care.
Use our experience to make it sure.

Contact us at www.exnit.com and www.eduexnit.pl

CS HUB

KRAKOW

THE PLACE WHERE CYBER MEETS SECURITY

THE KOSCIUSZKO INSTITUTE

WHAT **WE** DO?

In CYBERSEC HUB we believe that connecting means creating and that every network is more than the sum of its parts. That is why we launched our platform which brings together people from across boundaries. From the private to public sector, from the technical to political spectrum, we connect all those who want to forge a secure cyber future.

CYBERSEC HUB builds on the synergy between stakeholders from the Małopolska Region in Poland, with the city of Krakow as its strategic center. Krakow is one of the largest startup hubs in Europe with over two hundred ICT businesses, unparalleled investment opportunities, and access to talent, funding and the entire EU market. This unique environment is what attracts global IT companies to the area, many of whom have already moved their Research, Development and Security Operations Centres to Małopolska. Krakow also hosts the European Cybersecurity Forum CYBERSEC, one of the main public policy conferences on cybersecurity.

One of the initial projects run by our platform is CYBERSEC Accelerator which helps ICT and cybersecurity startups and SMEs from Małopolska to reach international markets. In the run-up to the project, an expert panel selected 7 of the most innovative businesses amongst the applicants. The Accelerator has been officially launched during the 2nd European Cybersecurity Forum CYBERSEC 2016. In this Innovation Book you will find unique products and services offered by CYBERSEC Accelerator participants.

The Kosciuszko Institute is a Polish think-tank founded in 2000. As an independent and non-profit organization, it gives itself the mission to contribute to the social and economic development of Poland in the European Union and as a partner of the Euro-Atlantic Alliance.

The experts of the Institute regularly cooperate with national and international organizations in the process of policy-making and initiating public debate on strategic issues.

Among its various areas of research, the Kosciuszko Institute leads its flagship projects in the field of cybersecurity, among them CYBERSEC HUB and the European Cybersecurity Forum – CYBERSEC.

We invite you to follow our initiatives and get involved.

Kraków, Poland.

www.ik.org.pl

THE KOSCIUSZKO INSTITUTE

is the publisher of

EUROPEAN CYBERSECURITY MARKET