Eleven Paths

WHITEPAPER

Cybersecurity Trends 2019

11.04.2019

Telefónica CYBER SECURITY UNIT

elevenpaths.com

Contents

1. Executive summary

Every new year provides a new opportunity to look through all events that took place over the previous year as well as to look ahead some of the issues that will engage us over the following year. In 2019, from ElevenPaths ─the Telefónica Group's Global Cybersecurity Unit─ we wish to take advantage of this time to analyze threat evolution in the digital world, new challenges before us and the way industry actors are meeting these changes, as well as to highlight those areas that from our point of view must receive greater attention over the following months.

Risks derived from the spread of digital transformation to companies and people's everyday life continue reaching high relevance. Thus, the need to adapt security to new ways of deployment, management and operation that arise as a result of cloud implementation and the concept of DevSecOps is taking on major importance. E-mail-related risks is increasing as well, with more complex attacks addressed to the increasingly ubiquitous IoT devices. Their protection requires the development of adapted security solutions or even specifically designed for this kind of devices. Even so, users' awareness and education remain critical to protect individuals and companies.

Conversely, an increase in the attacks on companies based on their partners' weaknesses compels us to extend the scope of risk management and to embrace new tools intended to analyze and automate those processes that make it possible to know and manage these increasing risks.

In light of this outlook, traditional perimeter-based security is called into question, so compelling us to take in 0-trust strategies and post-breach detection. Additionally, awareness of how inevitable is to suffer an attack is increasing, and sectors such as the insurance industry is meeting the demands through offers adapted to the different types of companies.

Concerning the CISOs, the need for solutions that provide a holistic view of risk remains, such risk being understood and managed in terms of business. Furthermore, complex attacks previously limited to states and critical infrastructures are now broadened to further organizations, and online fraud breaches the financial wall to reach other sectors. This scenario leads us to strengthen protection over private information. However, this aspect remains a challenge, particularly in international environments. Moreover, the lack of skilled professionals continues being a significant constant that hinders adaptation of companies for an environment where threats are increasing in terms of number and complexity and budget cannot keep pace with it.

The industry is trying to address all these issues and provide new solutions, such as the Managed Detection and Response (MDR) services ─that allow any company to profit from an advanced cybersecurity─, or the Digital Risk Protection (DRP) solutions ─that protect companies' digital exposure and are being increasingly implemented─. Threat Intelligence Platforms come also into play in their role of further step towards intelligence implementation, intended to improve the performance of any SOC.

Finally, we continue working on the use of machine learning as a technique to build a better protection intelligence against threats, but it is necessary to analyze more deeply its criteria and methods of implementation as well as to extend the scope of use of artificial intelligence, not only to prevention and detection, but also to reaction.

2. Digitalization

Our everyday life digitalization processes are unstoppable. The huge transformation that we are living currently as a result of digitalization, both individuals and companies, continues modifying our behaviors and being added, sometimes almost imperceptibly, to our habits and ways of doing. Nevertheless, these changes are above all necessary and irreversible. Many of the trends that we will see over this year have something to do with those changes, since they open the way to new threats and attacks.

2.1. Cloud implementation

Cloud implementation is important, even critical[1], to boost competitiveness and companies' positioning. Therefore, it constitutes a key element to the digital transformation process undertaken by most of the companies[2]. Within this new infrastructure and data management context, security emerges as the main challenge to be tackled, since deployment, management and operation processes concerning infrastructure and business implementation in hybrid, multi-cloud and SaaS environments require new controls as well as skill sets to be efficient.

In this sense, business units may deploy new infrastructure, such as code through agile processes, so that developers upload new versions of business applications that are critical for the company —every day, week or month to virtual machines and containers via DevOps processes. To this end, Continuous Integration/Continuous Deployment (CI/CD) schemes are used, that require the inclusion of new security controls in the workloads to protect business continuity without impact on productivity.

2.2.E-mail security

E-mail will remain the main cyberthreat vector for companies. More than 80% of the malware that touch companies do it via e-mail that, far from becoming outdated, is reinvented and exploited by cybercriminals by means of new and more complex techniques and methods intended to compromise their victims. In addition to usual malware, such as the ransomware that caught on in recent years, we are facing the Business Enterprise Compromise (BEC) —also known as "CEO Fraud"—, a type of targeted phishing that is growing significantly and bringing about higher losses for companies than the ransomware[3] itself.

Protection against this type of threats using e-mail and causing economic, productivity or reputational losses requires joining up employee's awareness on risks and appropriate behaviors when using e-mail systems that minimizes the risks for the company to be affected, to an e-mail security solution that makes it possible to detect these threats and protect companies and users against them.

2.3.People are the weakest link in the information security chain

Despite the level of investment in security solutions that has been reached in recent years, there is still a high number of attacks that are successful because of people's carelessness or lack of cybersecurity awareness. The efforts to educate people and ensure a high level of awareness and alertness among all the staff must be one of the greatest priorities for organizations.

[1] (1)13% of organizations that have implemented, or plan to implement, a digital transformation strategy state that, to this end, the cloud is critical; an additional 80% claim that it is important.

[2] 72% of organizations are planning to launch digital transformation strategies for next 2 years.

[3] https://www.muycanal.com/2018/08/03/empresas-timo-del-ceo-bec (in Spanish)

2.4. Internet of Things (IoT)

Internet of Things (IoT) is another trend connected with digitalization. Like all the other ones, it affects both individuals and companies.

2.4.1.B2C Digital Home

A growing presence of IoT devices at home will make these devices become a relevant attack vector for domestic users. This new focus of risk will be coupled with the continuing growth of malware and phishing from mobile applications. There will be also a growing trend to add a security layer and parental control at home through specific devices —or from the operator's network itself, that provide these functionalities to all devices connected to the domestic Wi-Fi without having to download specific protection applications.

2.4.2. Making device identification and authentication simpler

As consumers and companies are embracing more IoT devices and joining the network, the IoT ecosystem and its protection are becoming a hard task. In 2019, the need to provide solutions that make the onboarding process simpler, so facilitating IoT devices' identification and authentication in a simple and scalable way, will be more evident.

2.4.3. Increasing number of incidents affecting or involving IoT devices

IoT is an increasingly evident reality in the business sector that is blurring the concept of security perimeter among companies, so making traditional perimeter security systems less effective. For this reason, intrusion/threat detection is becoming necessary, requiring the development of specific solutions for those environments. In this sense, it is essential to generate specific cyber intelligence on IoT devices. Consequently, the emergence of systems contributing to this, such as IoT devices' honeypots, is foreseen. These systems collect attacks targeted on these types of devices and help to obtain this type of specific intelligence, that may be used to feed multiple security solutions.

3. Evolution of threats due to environmental changes

We do not only see attacks related to digitalization processes, but threats also evolve due to environmental changes.

3.1.Third-party cyber risk management

In 2018, we have observed several attacks based on the exploitation of vulnerabilities of third parties working with the target company. For attackers, from the business point of view, it makes totally sense: in a highly interconnected world, the security of any organization is as good as its weakest partner's one.

Within the maturity process of companies in terms of security, they face the new challenge of managing those risks derived from their relations with third parties. Traditional techniques based on surveys, audits and legal instruments remain valid in some cases, but they are neither scalable nor capable to provide all the necessary information to manage this type of risks.

New tools based on analyses and automated cybersecurity evaluations are emerging as an effective way to know and manage third party-associated risks at all stages of the process, from onboarding selection to continuous monitoring over the entire contract period.

3.2.Cyber insurance: protection network and driver of a better cybersecurity

So far, cybersecurity in its risk-associated facet has been focused on prevention, detection and response. These are valid and necessary; however, they are increasingly clear deficient approaches, since breaches and damages will inevitably occur within any organization.

In an era when all businesses are being digitalized, relying on a security insurance is a business requirement. A number of services and products are being developed on the cyber insurance market, giving coverage to large, medium and small companies and individuals. For years to come, cyber insurance will play a major role to provide a security network to many businesses as well as the appropriate incentives for all sectors to improve their positions.

3.3.0-trust and post-breach detection: the next security border

Security practice is accepting that it is impossible to develop 100% effective defenses based on the secure perimeter premise with trusted systems and users. By accepting the fact that these secure perimeters cannot exist, a new paradigm is coming out in cybersecurity, based on least privileges, encryption, obfuscation, advanced visibility, analytics and incident response.

4. Cybersecurity management environment

Along last years, some regulatory and environmental trends are gradually modifying our obligations as well as the way we apprehend security needs. Some of these trends will remain significant along this year.

4.1. Relevance of privacy and personal data management

This does not only apply the European area, but also other countries and regions that are updating their data protection and compliance models, including some issues already covered by the GDPR and that therefore make regulatory compliance in international environments difficult.

4.2.Unified vision of how security impacts business

There is a growing need for security programs to prioritize and report the business on its situation, which involves talking in terms of risk and having this information available, in real time and applied to each business process as far as possible. This will be one of the key aspects in cybersecurity management.

4.3. Attackers' capabilities reach levels previously reserved for states

Over last year, we have seen an increase in the activity of some states' actors, intended to the theft of intellectual property, trade secrets or other type of confidential information from trading and private organizations. Moreover, the level of tools and services modelled on techniques that before were exclusively available to states has become considerably sophisticated, so now they are easily accessible on forums and dark web markets. For this reason, CISOs must focus their efforts on those attacks that before only could be seen by governments and critical infrastructures.

4.4. Online fraud is no longer a bank's exclusive concern

Traditionally, online fraud has been considered a concern of banks and financial institutions. However, due to the speeding up of digital transformation among companies, and the migration of business and interaction channels to online environments, fraud starts being a huge concern for other sectors as well, such as e-commerce, mobile commerce, travel companies, etc. Even individuals must take identity theft seriously, monitoring their accounts and the publicity of their private information, in the face of potential information disclosure and third-party data leakage.

5. Managing talent shortage

Cybersecurity market continues to increase, and its growth is surpassing the global economy. In this context, the raw material is the talent. In the European Union (EU) alone, 825,000 professionals are expected to be required until 2025. On a global basis, (ISC)^2 forecasts 1,8 million in 2022.

This growth causes two opposed situations that will continue to define the market dynamics during this year:

1. A highly competitive labor market
2. An increase in technological investment to counterbalance the shortage of skilled professionals

Competitiveness in the labor market results in a year-over-year wage growth of up to 11%, with greater demands, not only in terms of salary, but also in global terms, particularly regarding the compensation and benefit packages, such as teleworking, working time flexibility or medical insurance. Some figures show that profile applications are doubled and recruiting processes are increasingly longer due to the challenge of finding the appropriate professionals.

- The most demanded profiles include CISOs with management and technical skills, who to a large extent will be postgraduate in cybersecurity or similar.
- Security Architects with deep knowledge of network architecture design, technologies of the major manufacturers and previous experience in network security.
- Pentesters and/or Senior Ethical Hackers with more than five years of experience and knowledge proven by the main certifications such as OSCP or CEH, and multidisciplinary experience in forensics, code analysis, or malware reversing.
- And, as the GDPR maturity process goes on, the demand for privacy consultors and Data Protection Officers keeps increasing.

In this sense, a high number of organizations are turning to their trustworthy service providers asking for CISOaaS or DPOaaS, outsourcing cybersecurity and data protection management, so that the talent shortage challenge may be overcome.

6. Evolution of protection solutions

Fortunately, significant developments have been observed along last years in terms of protection solutions. We will see their maturity process over this year, as well as how they will join the tools supported by security managers.

6.1. Digital Risk Protection solutions are increasingly omnipresent

"Security pros are turning to digital risk protection (DRP) solutions to deal with the heightened exposure their organizations' digital infrastructure, assets, and accounts face online."[4]

This is a new category of solutions that allow companies to protect their digital exposure, through assets outside their perimeter, digital identities used in social networks or different digital channels, or even through other type of information that, once on the Internet, may be exploited by malicious actors for their attack campaigns. These solutions cover from the protection of the brand and senior executives' identities to researches on the dark web.

These solutions allow to discover and monitor these digital assets, provide prompt remediation capabilities against attacks and protect the company's reputation and brand on the communication channels.

According to Forrester, 77% of clients consider DRP as a new solution which takes its place beside the set of tools that provide insightful information in their risk intelligence arsenal[4].

6.2. Advanced SOC capabilities for everyone

Cybersecurity industry is facing two opposed realities: on the one hand, it is necessary that all the organizations increase the level of sophistication of their defenses in order to be protected against increasingly advanced threats. On the other hand, there is a huge shortage of experts —and budget, even if growing, remains limited. For these reasons, building an advanced cyber defense is far from most companies' capabilities.

The industry addresses this need with a new generation of managed security services known as Managed Detection and Response (MDR). MDR services provide a full visibility of the devices and network, advanced post-breach mechanisms based on the detection of unusual or malicious behaviors, and threat intelligence; as well as an active and trained incident response service as part of the package. MDR is a cost-effective alternative that allow any company to be protected on the cyberspace.

6.3. From Threat Intelligence collection to its application

"Threat Intelligence" has been one of the trendy terms within the sector over last years. Nevertheless, a great number of companies that begin in this field have already noticed that collecting a high volume of threat intelligence is not enough, since this one may be really complex, volatile and hardly applicable outside the context of deep and specific researches performed by expert analysts.

For such reason, new tools and techniques capable to help any SOC to enhance its efficiency and effectiveness are emerging: by using a Threat Intelligence Platform, a SOC can match and prioritize all the tactical and operational threat intelligence received, and integrate it into the life cycle of all the SOC events, from detection and classification to hunting and incident response.

[4] The Forrester New Wave™: Digital Risk Protection, Q3 2018

7. Innovation for security

7.1. In 2019 we will not talk about whether machine learning must be implemented or not, but about how to do it

Machine learning is an old technique, but quite recent in the cybersecurity field. As any tool, if it is well implemented it may constitute a huge benefit. However, it might not always be the most adequate technique to solve a specific problem or it might not be correctly implemented. We believe that the correct implementation of intelligence systems is precisely one of the ongoing challenges to make machine learning an effective advantage and not just a simple advertising slogan.

For instance, in malware detection systems via machine learning it is essential to solve some issues in order to achieve a system rip enough to ease the burden of traditional detection systems based on signatures and heuristics. Much of the work to be done involves defining a line between the normal and the unusual.

If we stay in unmonitored methods to detect network anomalies or malware, it will be hard to discern what it is anomalous, and a great number of iterations will be necessary to perform a verification later. Consequently, a high investment in time and human assistance, or a purely "traditional" support for the analysis, will be required. We must observe the trends to realize if human assistance will be completely rejected or not, depending on the models.

In case of monitored methods, malware or network attacks' samples are already tagged according to the traffic, that go mixed over a machine learning box. A machine learning-based system success depends partly on the criteria considered to save and classify the samples used to feed that system. Even if a great number of fields have found the successful key, the remaining ones have not still achieved an exact solution.

7.2. From machine learning to AI

Machine learning may make it possible to build an intelligence capable to efficiently protect against threats. However, currently there is no debate over how to protect an equipment for it not to be attacked, but over how to respond appropriately when an equipment is compromised.

Therefore, although there is an increasingly work on the field of endpoint contingency, where normally security problems are gathered (or start), such field cannot be longer supported exclusively by signatures and traditional heuristic/dynamic detection. It is at this point where artificial intelligence plays a major role: as a key element, not only to preventive detection in sensitive systems, but also to reaction when the attack is carried out.

7.3. Persevering with identity and authentication

Identity and authentication remain network challenges, with clear signs of improvement. The fact that attackers have focused on second authentication factors means that they are being used more than ever, although it has highlighted their deficiencies as well. Authorization layers and advances in general are required when managing identity, both for users and machines. Moreover, these machines will be increasingly connected to the network with their own "identity" within the hive of IoT devices.

The rational model of traditional system's certification authority is being called into question: even if it is a trustworthy system, it is deficient at the current time. More than ever before, a potential business, applicable not only to SSL/TLS, but also to other fields related to third-party identity trust —whether machines or humans— is emerging. This is a market that must be developed and standardized.

Identity and authentication cannot be discussed without going over privacy. Security and privacy must be counterbalanced, with protection solutions addressed to users that do not involve sharing sensitive information with third parties, since it may compromise their privacy.

7.4. Security miniaturizing

To be efficient, security must be agile, cost-effective and invisible. The challenge is again to bring current security solutions in devices having lower technical and computational capabilities than traditional desktop systems or smartphones, such as cameras or routers ─these are devices that, by definition, will not be much more powerful in the future─. We believe that there will be a high demand of this type of solutions to help keep secure such devices using current technologies, although always considering their limitations.

About ElevenPaths

At ElevenPaths, Telefónica Cyber Security Unit, we believe in the idea of challenging the current state of security, an attribute that must always be present in technology. We're always redefining the relationship between security and people, with the aim of creating innovative security products which can transform the concept of security, thus keeping us one step ahead of attackers, who are increasingly present in our digital life.

More information

www.elevenpaths.com
@ElevenPaths
blog.elevenpaths.com

Information contained herein is owned by Telefónica Digital España, S.L.U. ("TDE") and/or by any other entity within Grupo Telefónica or their licensors. TDE and/or any other entity within Grupo Telefónica, or TDE's licensors, reserve all industrial and intellectual property rights (including any patent or copyright) derived from or applied to this document, including its design, production, reproduction, use and sale rights, unless such rights have been expressly granted to third parties in written form. Information contained herein can be modified at any time without prior notice.

Information contained herein may not be totally or partially copied, distributed, adapted nor reproduced by any means without prior and written consent of TDE.

This document is only intended to assist the reader in the use of the product or service herein described. The reader is committed and required to use information herein contained for their own use and not for any other purpose.

TDE shall not be liable for any loss or damage derived from the use of the information herein contained, for any error or omission in such information, or for the unappropriated use of the service or product. The use of the product or service herein described shall be regulated in accordance with the terms and conditions accepted by the user.

TDE and its trademarks (or any other trademarks owned by Grupo Telefónica) are all registered trademarks. TDE and its subsidiaries reserve all rights over these trademarks.