GLOBAL CYBER SECURITY CENTER

Newsletter

2019 April

Cyber Security is our mission

editorial

Be ready

In this digital context, the defense of information assets from cyber-attacks is increasingly playing a fundamental role.
All organizations that operate successfully in the digital sector must necessarily implement all the tools and actions that can prevent such attacks by guaranteeing data integrity and operational continuity, as cyber-attacks often undermine their continuity.
Bear in mind that the issues of Cyber security have been defined, by the European community, as the second emergency after climate change and before the current immigration issues.
In this context, it is essential to guarantee continuity of services and it is no longer just a question of compliance. Many institutions must, in fact, have business continuity plans, to comply with the regulations that impose it.
In the digital world this approach is certainly reductive, these plans must be present and predict also, cyber scenarios in addition to adverse situations such as natural disasters, plant failures, sabotage, pandemics, etc.
The business continuity plan must be structured with a series of processes that guarantee the resilience of all the essential functions for the organization's business. Allowing the identification of events and the management of incidents capable of compromising operational continuity by defining a structure that can react promptly, a structure that will require a multidisciplinary approach with the aim of reducing the risks related to this issue.
It is therefore necessary that the actions aimed at mitigating cyber threats adopt strategies that are in connection with the business continuity system, so as to guarantee, in the event of cyber events, that the organization can respond in a timely manner and with a series of plans and coordinated action.
An integration that must also include the aspects indicated by the European Privacy Regulation (GDPR).
In the digital domain, business continuity management, therefore, becomes a strategic process connected to Information Security issues.
It is essential that these plans are supported by technological platforms and coordinated at centralized level by SOC / CERT structures within the organization. Moreover, the concept of readiness needs to grow in digital organizations also through specific test that may involve also the C levels.
All these themes must then be included, also, in awareness campaigns.

Enjoy the lecture…

Nicola Sotira
General Manager GCSEC

events

Cybersecurity Mediterranean Congress - 2nd Edition
Location: Florence, Italy
Date: May 9-10, 2019
https://cybersecurity-mediterranean.it/
The Second Edition of the Cybersecurity Mediterranean Congress will be held in Florence, organized in collaboration with the GCSEC Foundation, Thales under the aegis of ITU, and under the patronage of the Swiss Embassy in Italy

ItaliaSec Summit
Location: Rome, Italy
Date: May 14-15, 2019
https://cyberseries.io/italiasec/
ItaliaSec returns to Rome for the third edition. It's an annual forum for the leading experts in information security, for both the public administration and the enterprises, in the Financial, Retail, Energetic, Chemical, Pharmaceutical, Manufacturing, Food, Health and Transportation field. Among the key topics for 2019: the interaction between the CISO and the Board, the process of ICT risk management and how to structure it in an organic way, the ROI on IT security investments, the creation of a corporate security culture, the cyber security of Operation Technology systems in a context of Industry 4.0

European 5G Observatory – Is Europe ready for 5G?
Location: Bruxelles, Belgium
Date: May 17, 2019
https://ec.europa.eu/digital-single-market/en/news/save-date-european-5g-observatory-europe-ready-5g
The stakeholder workshop "European 5G Observatory – Is Europe ready for 5G?" will take place in Brussels (Conference Centre Albert Borschette) on Friday, 17 May 2019 from 10:00-16:00. The workshop will be the opportunity to review the main findings of the first phase of the 5G Observatory and discuss the next steps to ensure the implementation of the 5G Action Plan.

in this issue

The information sharing and collaboration in assessing new Cyber risks

by Marco Fiore - GCSEC

Traditionally, an organization is management distributed information along a well-defined, top-down channel. Today, due to the spread of social technologies, information can be shared with great ease. This is why information sharing nowadays represents one of the main pillars of threat intelligence. Indeed, a good threat intelligence satisfies four main properties, also known as CART: **C**ompleteness, **A**ccuracy, **R**elevance, **T**imeliness the same properties that we could ascribe to information security sharing.

But the real effectiveness of all these conditions is obstructed if all players in the corporate world do not cooperate for facing new threats. Indeed, the posture of cyber security has been greatly weakened by an increasingly asymmetrical struggle. The boundaries, which have by now become unstable and immaterial, are threatened by attackers who have no face but have new effective tools to compromise day after day the whole business. It is necessary to opt for a more strategic view of these new scenarios and information sharing is one of the most effective tools for approaching new threat mitigation strategies.

As previously anticipated, if first the information sharing was a top-down corporate process now according to the new risk prevention logics is a process that moves transversely through its own company but also among all companies and that impacts the whole business. In the global and interconnected cyber world the organizations are called upon to face threats that are constantly evolving. Sharing of information, knowledge and experiences about new threats and procedures and instruments to prevent and react to them can help all organizations to improve their defence capacity and cyber security posture.

Given the real complexity that today's companies are facing and will have to face the importance of cybersecurity specialists is crucial. Only an early detection and a strong response capability can help organization to face cyber-attacks. If we consider immediate response in the event of an accident as the main objective of the SOC E CERT and CSIRT, the human factor continues to be the glue between knowledge and technology and the vanguard of the cyber threat.

Exceedingly, in a world flooded with billions of information and data, the human factor continues to be the essential element for extracting knowledge from this enormous amount of data.

Open sources and information available of the single organization on their own no longer provide guarantees, especially as the growing need to share information on threats and attacks suffered represents an important prerogative for the defense of perimeters that are no longer physical or mainly perimetral. The cloud amplifies this perimeter dimension.

news

Qrypter is evolving, it's confirmed by a targeted campaign in Italy

https://www.difesaesicurezza.com/en/cyber-en/qrypter-is-evolving-its-confirmed-by-a-targeted-campaign-in-italy/

Yoroi-Cybaze Zlab: The Qrypter malware, a MaaS usually launched in combination with AdWind/jRAT, is evolving. A targeted campaign in Italy reveals a new version, capable to be invisible for several antivirus engines. Qrypter malware is evolving. It has been confirmed by Yoroi-Cybaze ZLab cyber security experts, who analyzed some malicious emails, sent to a very few organizations and with the contents specifically tailored for Italian speaking targets. the malicious code is a Malware-as-a-Service (MaaS), especially popular for its usage in combination with AdWind/jRAT. However, the new sample seems to exhibit different protection techniques with respect to the previously documented ones. Most files are encrypted and only one of them represents an runnable Java Class. It contains a Java Main, responsible for decrypting and launching the actual payload.

New Apache Web Server Bug Threatens Security of Shared Web Hosts

https://thehackernews.com/2019/04/apache-web-server-security.html

Mark J Cox, one of the founding members of the Apache Software Foundation and the OpenSSL project, today posted a tweet warning users about a recently discovered important flaw in Apache HTTP Server software. The Apache web server is one of the most popular, widely used open-source web servers in the world that powers almost 40 percent of the whole Internet.

The vulnerability, identified as CVE-2019-0211, was discovered by Charles Fol, a security engineer at Ambionics Security firm, and patched by the Apache developers in the latest version 2.4.39 of its software released today. The flaw affects Apache HTTP Server versions 2.4.17 through 2.4.38 and could allow any less-privileged user to execute arbitrary code with root privileges on the targeted server.

Artificial intelligence: Commission takes forward its work on ethics guidelines

http://europa.eu/rapid/press-release_IP-19-1893_en.htm

The Commission presents today next steps for building trust in artificial intelligence by taking forward the work of the High-Level Expert Group. Building on the work of the group of independent experts appointed in June 2018, the Commission is today launching a pilot phase to ensure that the ethical guidelines for Artificial Intelligence (AI) development and use can be implemented in

But information sharing, therefore, means also to "establish an organizational and technical infrastructure that encourages free exchange but also enforces controls that mitigate the risks of irresponsible use."[1]

The characteristics of info sharing have been transformed from simple information sharing to sharing practices and methodologies. The secret is not closing like a hedgehog but creating a conscious sharing of information and threats in order to be always ready to face the news and new threats of the IT landscape.

Based on the considerations made so far, the project that GCSEC is conducting with its CERT STAR PROGRAM is certainly a good way to improve the information sharing and collaboration between cyber security teams.

The awareness of being able to learn and deepen new knowledge during the meetings is certainly one of the added values of the program. In the same time it is good to keep in mind a fundamental paradigm: to make a common market that sees all the companies involved in facing global cyber threats, it is unthinkable to do it selfishly. It is necessary instead to implement common policies of exchange and sharing information in order to be even more resilient to threats that are not already known to take correct proactive measures.

This type of meeting are dedicated only to analysts and operators of Italian CERTs and SOCs of Critical Infrastructures, Institutions and Public Administrations. It aims to enhance competences, improve cooperation and experiences exchange between security teams. The information exchanged allows groups of expert essential to have a holistic and effective approach to new threats and enhance defense capabilities of each one.

Without prejudice to the need of companies to recognize among their prerogatives the need to maintain classified and confidential information, this exchange can include both internal and external information that help cyber-specialists to collect each other new points of view to approach problems from different perspectives.

Fundamental elements at the base of a sharing process are also represented by the level of maturity of the receiving organization and the trusted source from which the information comes. In those groups in fact CERT and SOC's cyber specialist could share relevant information on how companies approach threats in their organization.

Those workshops are divided in two main moments. A first one dedicated to analysis of specific issues (for examples threats or attack's techniques) a second one more practical with hands-on exercises and the use of the main tools and technological platforms.

The focal aims of those meetings are:

• Increase a shared situational awareness and the perception of what we are going to do on cyber threats;

• Share best practices in threats prevention and detection

• Identify changes in the short and long term;

• Put together in a systematic way the intervention teams to self-evaluate their cyber-posture and favor the questioning and overcoming certain mental schemes that are harmful to the intervention;

• Enhance trust and cooperation between cyber security teams of different organization;

• Be prepared in quiet moments constituting a critical review of aspects neglected or unknown creating new knowledge.

The CERT STAR PROGRAM therefore represents an indispensable moment for enhancing intelligence activities, allowing to analyze, for each specific market sector, technically the issues of the complex panorama of threats.

It has become necessary not to interrupt the process of enriching and sharing this information by working, as GCSEC has done for years, on the construction of solid and formalized interconnection channels between the different internal and external company departments to facilitate information exchanges between different national and international public and private organizations.

practice. The Commission invites industry, research institutes and public authorities to test the detailed assessment list drafted by the High-Level Expert Group, which complements the guidelines. Today's plans are a deliverable under the AI strategy of April 2018, which aims at increasing public and private investments to at least €20 billion annually over the next decade, making more data available, fostering talent and ensuring trust.

'Highly Critical' Unpatched Zero-Day Flaw Discovered In Oracle WebLogic

https://thehackernews.com/2019/04/oracle-weblogic-hacking.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29

A team of cybersecurity researchers today published a post warning enterprises of an unpatched, highly critical zero-day vulnerability in Oracle WebLogic server application that some attackers might have already started exploiting in the wild. Oracle WebLogic is a scalable, Java-based multi-tier enterprise application server that allows businesses to quickly deploy new products and services on the cloud. It's popular across both, cloud environment and conventional environments. Oracle WebLogic application reportedly contains a critical deserialization remote code execution vulnerability that affects all versions of the software, which can be triggered if the "wls9_async_response.war" and "wls-wsat.war" components are enabled. The vulnerability, spotted by the researchers from KnownSec 404, allows attackers to remotely execute arbitrary commands on the affected servers just by sending a specially crafted HTTP request—without requiring any authorization.

New Emotet trojan variant uses different POST-infection traffic to infect users

https://cyware.com/news/new-emotet-trojan-variant-uses-different-post-infection-traffic-to-infect-users-a004274a

A new variant of Emotet trojan that leverages a new POST-infection traffic technique has been discovered recently. The malware variant is tracked as Trojan.W97M.POWLOAD and spreads via phishing emails. How does it propagate - According to researchers from Trend Micro, the new sample spreads via spam email with the help of the trojan downloader Powload. The email contains a malicious ZIP file, which if opened, results in the download of the malware. In order to open the file, the victims are required to provide the 4-digit password which is included in the email. What's the change in POST-infection traffic - Unlike the previous version, the new variant uses random words and numbers as a URI directory path in order to evade detection.

[1] Roland Deiser and Sylvain Newton, Six social-media skills every leader needs, Article 2013
https://www.mckinsey.com/industries/high-tech/our-insights/six-social-media-skills-every-leader-needs

Multidisciplinary incident management

By Massimo Cappelli - CERT, Poste Italiane

The management of an incident is the most critical task that a Computer Emergency Response Team (CERT) or a Security Operations Center (SOC) can tackle. When dealing with an accident, there are many factors to consider and the time required to take them into account is reduced. To this must be added the element "*stress*" that affects the performance and choices to be made.

For the latter reason, we always remember that it is essential to prepare for the event. The management of an accident cannot be improvised. The *table top scenarios* to oil the aspects of collaboration and communication and the exercises, to test the procedures of the departments involved, should be carried out annually to verify each aspect of management and improve its effectiveness and efficiency. The procedures serve to reduce the time of "psychological blockage" that affects those involved in management.

Unfortunately, these activities are underestimated because they are considered to have a low added value. The departments involved are many and the agendas of managers are often misaligned and do not allow common moments of comparison and testing. This has a major impact on the timing and response to an accident. Starting to handle an incident the moment it's identified, it's too late. As in the Civil Protection and Defence manuals, also in cyber security the key concept is readiness or "*preaparedness*", which is achieved only with preparation.

Some of you will wonder about the relevance of the introduction to the title of the article. The answer is everything. We consider the macro-process of an incident management and we verify how fundamental is the preparation as well as the multidisciplinarity.

The first step is to identify an accident. An incident can be reported by a customer, an employee or identified during the service monitoring phase.

The first activity to be carried out is a quick triage to understand what is happening and what the impact on services can be in terms of interruption, loss of confidentiality, integrity and availability (RID) of information but especially in terms of economic impact. Speed is essential to determine impact, but it's not something you can do on the spot. The impact is determined on the basis of considerations made during the **preparation phase**. Usually an **impact matrix** should be used where different evaluation parameters (e.g. personal injury, service interruption, RID compromise, economic loss, image loss,...) and different criticality levels (e.g. green, yellow, orange and red) are considered. On the basis of the triage, the severity of the event must be determined, from which the actions to be implemented will arise. This is why multidisciplinarity comes into play as early as the assessment phase of the accident. To be more precise in the preparation phase to draw up the impact matrix for the evaluation of the accident. The actors who must be involved at the table, in addition to the technical profiles, are certainly the "*business owners*" of the service, the *data protection officer*, the department of communication / public relations, *customer care*, legal and regulatory affairs. All these figures must jointly identify which are the criticality levels (thresholds) for each individual parameter of their relevance. For each level of criticality a specific procedure of intervention will be established, involving other structures and levels of management and internal and external communication.

The thresholds must be quantitative and not qualitative. The potential impact, defined on the matrix, determines, as already mentioned, the actions to be carried out. If the impact is smaller, it is usually managed within the SOC/CERT technical structure/presidium. The situation is different where the impact is higher in terms of inefficiencies, economic or reputational losses. In this case, an incident management procedure involving several structures is initiated. Multidisciplinarity has its maximum expression during a **crisis** in which several concomitant factors must be managed. Leaving aside the purely technical IT and security aspects of accident management, I shall present below some of the **disciplines** that should be involved in the resolution of the crisis.

First of all, the ***business owner of*** the service. The *business owner* is the one who can best describe the direct impact of a disruption or blockage of its service and translate it into economic losses (lost revenue, production deadlock, slowdowns, ...). The *business owner*, during the crisis, must already have estimates of what the impacts may be based on the time for which the disruption is slowed down or stopped. For this reason, I would like to stress that most of the activities must be carried out during the "peacetime", as well as the collection of all the information necessary to understand the scope of the event. The more you have a view of detail, the better. If it

is possible to determine the flow of revenues deriving from the service, based on the history of previous years, in terms of reference period (days, hours, etc. etc.), the greater the accuracy of the estimate will be. Obviously for new services, the estimate will have to be based on a methodology. Some might even argue that it is not necessarily the case that each period is the same as the previous year. That is true, but if you don't have any other methodology to base yourself on, we should start somewhere.

Another aspect and discipline to consider is certainly communication. Communication plays a key role in accident management. If you communicate badly or late you risk the amplifying effect of the impact. In the event of an accident, it is advisable to communicate first and not wait for the voices to leak out and be interpreted or distorted. The risk is the effect of the game "Catch the mole" i.e. you spend your time denying instead of being a primary source of information. The main factors to consider in communication are the **messages** to be conveyed and the **channels** to be used according to the type of *stakeholder* (*target*) to be informed. Communication could be institutional and therefore use a more formal or customer-oriented format and therefore use simpler terminology.

Communication, however, is meek if you do not know the *target* to which to communicate. This is where two other disciplines come into play: *customer care* and psychology/sociology/anthropology. *Customer care* is essential to get to know your customers or investors. Factors such as age, geographical area of belonging, preferential channels for information, type of product / service acquired are useful to understand **which channel** to use and the frequency with which they need to be updated. Psychology/sociology/anthropology, if I have condensed them into a single group, is useful to understand **which message** to communicate. Different types of customers may need different messages that can be understood by the customer. Psychology is used to define an effective message that produces the desired effect (soothing, alerting,...). Sociology/anthropology is necessary to understand the effects of the accident. A crisis can produce knock-on effects, such as indignation, consensus, frustration, which spread within social groups in different ways. The leakage of personal data may be experienced differently between a group of teenagers and a middle-aged group or between peoples of different cultures.

In addition to the communication aspects, the contractual aspects relating to customers are also relevant. If Service Level Agreements have been defined, the Business and Legal functions must determine what the direct consequences may be. Whether there are specific performance clauses to be guaranteed, whether there are contractual termination clauses, or whether there are particular indemnities to be taken into account, will therefore be decisive in both the impact definition and the resolution phases. It is important that this information is available already at the stage of impact analysis because it should be considered within the matrix but often it is not.

The Regulatory Office, like that of the Data Protection Officer, should be called upon to determine whether any incidents were caused by the company's failures and whether these failures, in addition to requiring specific notifications to the relevant public officials or customers themselves, do not provide for potential sanctions.

Finally, the presence of the Purchasing Department should also be considered. The resolution of an incident may require the activation of extra-budget contracts and the method of acquisition must be defined and formalized by the purchasing department in derogation of internal procurement policies.

These are just some of the functions that, in my opinion, should be triggered during a high-level crisis or incident. In conclusion, I would like to reiterate some of the fundamental elements of accident management: defining a holistic accident management process; defining an impact matrix as detailed as possible; defining the rules of engagement on the basis of the criticality levels of the matrix; testing the communication flows between the various departments; carrying out periodic exer exercises; preparing different accident scenarios with related response procedures. All this must be prepared in peacetime and therefore requires the collaboration of all functions. In the future, Artificial Intelligence may change the response time and also the relevance of some functions compared to others, but we will deal with it on another occasion.

Continuity comes from resilience, resilience comes from readiness, readiness comes from preparation, preparation from *commitment*.

Let's remember that a mismanaged incident affects everyone's business objectives.