Incident Response as a Key Factor of Defense

MILICA D. ĐEKIĆ, Subotica

Professional paper

UDC: 007:004.056.5

004.6.056

DOI: 10.5937/tehnika2006809D

According to the ancient Chinese learning our world is governed by two opposite forces being Yin and Yang. Those forces are the force of offense and force of defense and by the same doctrine our world can be in harmony only if those two forces are in balance. The modern security experts would also see a security as a balance between attack and defense. So many defense professionals worldwide would approach their everyday tasks with such an assumption. The similar situation is with the cyber defense – the cybersecurity researchers and practitioners would see cyber defense as a balance between cyber attack and its defense. Also, this doctrine would get led with the theory that there are some passive and active principles in cyber defense. For instance, the passive principals are cyber prevention and monitoring, while the active principle is the incident response. The ongoing experience would suggest that the majority of marketplace actors would invest a lot into the passive factors of cyber defense, while the incident response would get less used due to some objective and realistic parameters. The main concern with the incident response is that it requires a lot of skills and expertise in order to get applied. There is the entire flow in a cybersecurity that would suggest that all three indicators of the cyber defense passive and active principles should get equally distributed. In addition, coping with such a concept so many cyber experts would see the incident response as a key pillar in a cyber defense. In this effort, we intend to provide a deep insight into such learning as well as provide some comments and discussions coming from our own research experience.

Key words: incident response, cybersecurity, skills, intelligence

1. INTRODUCTION

As it's well-known, cyber defense would deal with so many practical variations depending on the organization it got implemented in. For example, the large scale companies would usually cope with the security operating centers (SOCs), while the small businesses would suffer a certain lack of cybersecurity procedures and policies. [1, 6, 7] So many laics would believe that the small businesses are not an attractive target to the hackers, but the studies would suggest that the cybercrime underground would make the biggest profit affecting the small businesses. What is the trick? The small businesses would usually deal with a poor cyber defense and they would not know how to tackle the incidental situation at all. Also, they would be the critical infrastructure to many economies for a reason they would get a dominated form of enterprises. The

hackers would get aware of that and they would target those organizations mostly and frequently. The logics got quite clear – you would get an opportunity to make the good money and you would expose yourself to the minimal risk. Who would reject such an adoring offering?

On the other hand, the large companies would mainly use so expensive and sophisticated SOC's and they would undoubtedly know how to tackle such a problem. The cyber criminals aiming to do something spectacular would see as a challenge making the breach to such an asset. They would know that such an action could bring them the huge profit as well as attract the attention of so many media houses giving them some kind of publicity and in case of different age groups – maybe some sort of popularity. So many teenagers and young people would dream to live such an exciting life and they would latently be on the side of the bad guys committing those sorts of the crimes. In our opinion, it's so important to share with the public the experiences of law enforcement officers and cybercrime investigators in order to make people understand how thrilling and dedicating those roles

---

Author's address: Milica Đekić, Subotica, Vase Pelagića 39a

e-mail: milicadjekic82@gmail.com

Paper received: 18.11.2020.

Paper accepted: 24.11.2020.

are. [2, 5] In other words, the popularization of defense and intelligence professions is from a strategic importance for the future of any society in the world.

In the practice, so many organizations would depend on the cybersecurity prevention solutions such as anti-malware software. Also, in the case of monitoring – the SOCs would rely on the analytics tools, so far. There are some concepts in a security community that would suggest that we need more security professionals even in the small enterprises. One of the most famous such paradigms is the Enterprise Security Risk Management (ESRM) being developed by the ASIS International being the world's leading security association. That concept would indicate how significant the security is amongst any marketplace players for a reason that the lack of the best practice in defense and intelligence could cost as a lot. In addition, it's important to know that it's crucially helpful to prevent the cyber attack and if you are not able to do so, you should know how to minimize the consequences of such an event. [10, 11] The cybersecurity experts would agree that it's not the question if the breach would happen anyhow, but rather when it would occur. In other words, it's so important to accept the fact that the cyber breaches are inevitable.

2. THE BACKUP PROCEDURES AND POLICIES

Through this article, we would give a brief overview how important it is to accept the existence of cyber breaches in any environment. The cyberspace got the place of a modern battlefield and so many hackers, cyber criminals and cyber warriors would use so in order to conquer the new and new cyber territories. So, dealing with the fact that cyber breaches are happening every single day and no one got immune to them is so crucial in order to understand how to protect yourself and your asset from those attacks. The most ultimate challenge to the majority of IT security professionals is that they need to react somehow in order to respond to an incidental situation. Some military doctrines would suggest that if you know your enemy and yourself, you would get any war. Also, we would add that the good defense is about understanding the threat.

So, what could happen if the cyber incident occurs? First, you should know that the bad guys would deal in so many different ways and they would use so many different approaches in order to take advantage in the cyberspace. Either they choose to do some business espionage or the entire sabotage – the impacts are more or less similar. Your business would definitely cope with some kind of disadvantage. [11, 12, 14] In other words, the primary thing you should do in order to protect your asset is to develop the useful backup procedures and policies. Those documents

would include a set of advices and recommendations how to deal in case you lose some of your sensitive information. In other words, it's so important to save your data periodically in order to get in a position to return them once they got deleted from your IT infrastructure.

In order to make the backup procedures and policies you need so skillful cybersecurity professional who would assess the risk to your organization and prepare the helpful documentation that would so carefully describe how to cope with the certain situation. This sort of an activity is also the part of an incident response strategy because sooner or later anyone would suffer the cyber breaches and that organization should know how to resolve such a situation. The effects of successfully conducted cyber campaigns could get so harmful and the business not being capable to protect its sensitive information can lose its position on the marketplace. The professionals working on such tasks are usually the procedure and policies developers and those folks would normally cope with a plenty of experience in a cyber defense dealing with some cybersecurity certificates. The certification in security is so important because it would guarantee that someone has the sufficient experience to take some testings and through that exam gain the certification which must get renewed from time to time. Finally, the good cyber defense is about the good skills and rationally made decisions, so far.

3. THE BUSINESS CONTINUITY AND DISASTER RECOVERY

In a business world, time means money. For such a reason is crucially significant to get why any kind of business discontinuity could be so dangerous to any organization. The purpose of this effort is to make an open discussion why the incident response matters in a modern cyber defense. In so many cases, the people would not get aware how cyber attack would appear in the practice and by our research; they would not even get sure if they have ever gotten the target of hackers. For instance, through our career – we have interviewed some engineering experts about their experiences with the hacking attacks and they mainly got less confident if they have ever been hacked. Also, the engineering community would so commonly complain that its devices would so suddenly get broken and it would get a lot of spam and adware as well. So many folks would believe that the errors with their computers and networks are the consequence of the less competitive solutions they so often use in the private and business lives. [1, 13] This is only partially accurate because those professionals would not get aware of the risk coming from the outside. All these stuffs would affect our functioning at so many levels and we would not

recognize that they are the impacts of cyber attacks, so we would not apply the adequate incident response strategies and tactics.

In our belief, the handy way to avoid this kind of scenarios is to try to correlate your technology with a defense. If you notice that your machine is operating in a quite strange manner, it does not mean it's about the manufacturing flaw and you need to complain to your vendor immediately. Practically, it's about some sort of the flaw in your operating system or software and that sort of mistake would get called the vulnerability, so the hackers would know how to exploit that piece of a programming code. Right here, we would make a quite deep insight in order to make everyone understands how challenging and difficult the role of incident responders is. Those folks are still quite rare on the marketplace and dealing with the good incident responder is the real luck.

Being the incident responder would not mean that you would detect the cyber attack, terminate all suspicious connections from your network and backup anything getting lost from such an incident. In so many cases, that role seeks a lot of expensive skills such as programming, network administration, system engineering, troubleshooting and much more. After the only one cyber incident, your IT infrastructure could get left in a total chaos and in such a case; you need a team that would get capable to respond to such a disaster and return the business continuity on. From that perspective, it's quite obvious why the incident response and business continuity with the disaster recovery are from a key importance to each other. In some cases, if you suffer the lack of the good incident response, your business could never recover from the hacker's attacks and you would definitely need to quit with so. The incident responders are so smart and skillful guys who could do a lot of beneficial stuffs for any organization, so it's so significant to get them amongst your employees.

4. CYBER SKILLS SHORTAGE IN THE 21ST CENTURY

The cyber industry would greatly need the professionals who would meet its requirements. According to some sources, there will be the cyber skills shortage over the period of the next, say, two decades. The entire world got so dependable on the new technologies and in so many cases; it's not enough to be the skillful end user only – but, it's necessary to cope with much deeper understanding of such an area. The cyber industry would produce a plenty of courses and training in order to raise the preparedness of its members. Also, it's required to deal with the similar skills in the rest of the commercial branches. The IT security field could help us getting more competitive and productive,

that's why so many stakeholders would invest a lot of funds and efforts in order to take advantage over this new area of interest. [1, 2] Additionally, even the malicious actors got dependable on the emerging technologies and that's the reason more to take seriously that industry as something being strategically important for the international security.

In this historical period of time, we live in so complex and dynamic environment that would make us dealing with so many threats, risks and challenges. For those purposes, it's from a vital interest to accelerate our industry and commerce to start adopting the changes at the much faster pace. From such a perspective, the role of the incident response may appear as so critical because of its capacities to tackle, investigate and resolve the certain situations on. The most superior incident response teams would work in the high-tech surrounding and those guys would know how to protect the asset they are supposed to watch after. Finally, we should mention that the good cyber defense is a mix of the emerging technology and defense and in any case; beside you should cope with the laws and criminal justices – you should deal with the strong engineering skills as well in order to understand that super new technology.

5. INCIDENT RESPONSE SEEKS TO THINK LIKE A HACKER

As it's well-known, the hacker's community would be so responsible to any kind of cyber incident occurring in the world. In so many cases; the incident responders should get familiar with the ethical hacking and indeed; they would pass through so many educational sessions that would instruct them how to handle the hacker's tools. [1, 2] Once they learn to think like a hacker, they would show more results at their work and they would get capable to figure out what the capacities of their attackers are.

In other words, those incident responders would get confident about their knowledge and they would develop the skill through their experience to recognize their enemies, so they would frequently get the wars. This sounds as quite promising and as some saying would suggest the more you do – the better results you would obtain. In our belief, this could get the imperative to the next generation of the incident responders who should get able to resolve nearly any cyber incidental situation.

6. THE ECONOMICAL IMPACTS OF INCIDENT RESPONSE

There are some projections coming from the reputable sources that the cybercrime would cost us several trillion dollars per an annum in so close future.

This is quite alarming having in mind that's nearly 5% of the world's gross product. [12, 13, 14] In other words, if we do not respond to the incidents in the cyberspace and we leave the things like so – we could fail in the big trap that would keep us paralyzed for a quite long period of the time. In the worst case scenario, this could lead the human kind into the series of crises and definitely shake our economies, the entire progress as well as prosperity. As it's known, no society got isolated and everything happening somewhere would get reflected to its nearest surrounding sooner or later. No one would want to deal with the crisis management because it's so trickery discipline and those folks doing such a job would be an analogy to the incident responders and we could so confidently call them the crisis responders. Anyhow, any cyber incident is the crisis at a micro level that could run the entire avalanche of issues that could cause the catastrophic impacts to everyone.

7. DISSCUSIONS

The incident response could seem as so critical factor in a defense and practically, it is. Through this effort, we have discussed how the incident response could affect our safety and security and why it is significant to put a lot of effort on in order to tackle any incidental situation, so far. The prevention and monitoring could do a great job, but the incident response would appear as a key pillar to many.

For such a reason, we would want to highlight that any non-obtained incident response could mean the beginning of a crisis that could bring with itself so harmful implications. We believe that's the fact more to try to leverage your incident response team and make your IT infrastructure getting more resilient to any sort of offense.

8. CONCLUSION

The cybersecurity is not the new branch of science and technology. It would exist so many decades back and with the discovery of the first digital systems, the people would realize those advancements are not safe enough and there must be the ways to protect yourself and your asset from being offended.

The roots of cryptography being the vital area in any defense would go deeply to the ancient times of the European history. It would appear that even today the cyber defense is nothing new, but only the ongoing topic being the part of our everyday lives.

REFERENCES

- [1] Ablon L, Libicki M. C, Golay A, *Markets for Cybercrime Tools and Stolen Data*, Sponsored by Juniper Networks, 2014, Web source: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf
- [2] Beaver K, Davis P. T, *Hacking Wireless Networks for Dummies*, Wiley Publishing, 2005, Web source: https://cdn.preterhuman.net/texts/underground/hacking/Hacking_Wireless_Networks_For_Dummies_2005.pdf
- [3] Bergman M. K, *The Deep Web: Surfacing Hidden Value*, White paper, 2000, Web source: http://journal.ggn.com.br/sites/default/files/documentos/2011_bergman_7_cafarella_informationretrieval_presentation1_2.pdf
- [4] Charney S, *Rethinking the Cyber Threat: A Framework and Path Forward*, Microsoft, 2009
- [5] Chaliand G. and Blin A, *The History of Terrorism*, University of California Press, 2007, Web source: https://wikileaks.org/gifiles/attach/177/177597_History%20of%20Ter.pdf
- [6] CRS Report for Congress, *Critical Infrastructure and Key Assets: Definition and Identification*, 2004, Web source: <https://www.fas.org/sgp/crs/RL32631.pdf>
- [7] James P, Jenson M. And Tinsley H, *Understanding the Threat: What Data Tell Us about U.S. Foreign Fighters*, START, 2015, Web source: <https://www.start.umd.edu/publication/understanding-threat-what-data-tell-us-about-us-foreign-fighters>
- [8] *RFID Security*, The Government of the Hong Kong Special Administrative Region, 2008, Web source: <http://www.infosec.gov.hk/english/technical/files/rfid.pdf>
- [9] Payne S. P., *A Guide to Security Metrics*, SANS Institute, 2007, Web source: <https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55>
- [10] Puhe M, Edelmann M, Reichenbach M, *Integrated urban e-ticketing for public transport and touristic sites*, Final report, Science and Technology Options Assessment, 2014, Web source: [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513551/IPOL-JOIN_ET\(2014\)513551_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513551/IPOL-JOIN_ET(2014)513551_EN.pdf)
- [11] Ponemon Institute LLC, *2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute Research Report, 2015, Web source: <https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF>
- [12] Symantec, *Internet Security Threat Report*, 2016, Web source: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>

- [13]S. Weine and B. H. Ellis, *Lessons Learned from Mental Health and Education: Identifying Best Practices for Addressing Violent Extremism*, START, 2015, Web source: https://www.start.umd.edu/-pubs/START_LessonsLearnedfromMentalHealthAndEducation_FullReport_Oct2015.pdf
- [14]Weine S. and Ellis B. H., *Supporting A Multidisciplinary Approach to Addressing Violent Extremism*, START, 2015

REZIME

PROTIV-INCIDENTNO DEJSTVO KAO KLJUČNI FAKTOR ODBRANE

Prema drevnom kineskom učenju naš svet je pokretan dvema suprotnim silama Jin i Jang. To su sila napada i sila odbrane i po istoj doktrini naš svet može da bude u harmoniji samo ako su ove dve sile u ravnoteži. Savremeni bezbednosni stručnjaci takođe vide bezbednost kao ravnotežu između napada i odbrane. Jako mnogo profesionalaca u bezbednosti upravo pristupa svojim svakodnevnim obavezama na taj način. Slična situacija je i sa visokotehnološkom bezbednošću – eksperti u tom polju vide visokotehnološku bezbednost kao ravnotežu između visokotehnoloških napada i njihove odbrane. Takođe, ova doktrina je vođena teorijom da postoje i pasivni i aktivni principi u visokotehnološkoj bezbednosti. Na primer, pasivni principi su visokotehnološka prevencija i nadzor, dok je aktivni princip protiv-incidentno dejstvo. Tekuće iskustvo sugeriše da većina učesnika na tržištu ulaže mnogo u pasivne faktore visokotehnološke bezbenosti, dok se protiv-incidentno dejstvo slabije koristi iz nekih drugih razloga. Glavni problem sa protiv-incidentnim dejstvom je to što ono zahteva mnogo znanja i veština. Postoji čitava struja u visokotehnološkoj bezbednosti koja zagovara da sva tri pokazatelja principa visokotehnološke bezbednosti treba da su podjednako zastupljena. Dodatno, radeći na takvom konceptu jako mnogo istraživača sagledava protiv-incidentno dejstvo kao ključni stub u visokotehnološkoj bezbednosti. U ovom radu, pokušaćemo da pružimo dubok uvid u dato učenje, kao i da damo neke komentare i diskusije koji dolaze iz našeg ličnog istraživačkog iskustva.

Ključne reči: *protiv-incidentno dejstvo, visokotehnološka bezbednost, veštine, saznanje*