IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact Factor: 6.078

(Volume 8, Issue 3 - V8I3-1449)

Available online at: https://www.ijariit.com

Intelligent security response system

Suresh K. P.
kpsuersh@gmail.com
Independent Researcher

ABSTRACT

Secure product development is the mantra in having lesser vulnerabilities during the life cycle of a product. There are many well-known frameworks and policies companies have been following to ensure the same. E.g. Shift left security. While this being a proactive measure in ensuring security, the reactive support from the security response team also plays an equal role. The mission of any Security Response Team is to protect confidentiality, integrity, and availability of companies' & customers data by ensuring a responsible disclosure of security vulnerabilities reported by external / internal sources in the product portfolio and in services portfolio. Through this study an attempt is made to find out and list down the risks involved, if there is a deviation from responsible disclosures by external researchers and along with that exploring a technical solution that could help companies have this details of the risk, at first hand. The very reason to name this solution as "Intelligent Security Response System" is that it brings in that extra intelligence that sometimes slips out from normal proactive monitoring solutions. The solution also has the capability to intelligently identify risk ratings and filtering logic, from the historic data which gives it an upper hand in terms of quickly identifying and notifying a threat with a false positive. In the onset of the latest technological disruptions, and the bad actors using all means to exploit the product vulnerabilities, this study also intend to identify the possible shortfalls and opportunities of improvement.

***Keywords**: ISRS, Product Security, PSIRT, Responsible Disclosure.*

1. INTRODUCTION

Business are often faced with the challenges of addressing the vulnerabilities that are arising after a successful release cycle. Companies needs to be prepared for vulnerability reports received during productive usage. In such a case, they need to have contacts in place and the right technical skills available immediately to triage and investigate vulnerability reports and either confirm or reject the vulnerability. For a confirmed vulnerability, the company is requested to provide timely security corrections to sanitize the issue according to the severity based on the internal target. The product security response teams help in ensuring high-quality mitigation of the risk of security vulnerabilities in released software which is being productively used. Figure 1.1 explains the life cycle of a typical product vulnerability. Ideally starts with either from a surveillance / disclosure event which gets validated as per the established processes. This is to ensure that false positives are removed and avoid duplication with already triaged and in process findings. Such inputs of vulnerabilities can be submitted by customers, partners, or even security researchers. Companies usually will provide an encrypted channel to submit such inputs. This is normally called as the security inbox, which will be an encrypted channel. Submission of an entry here triggers a workflow to the psirt teams. Industry data shows that close to 93 percent of deployments had misconfigured storage services, which lead to the exposure of more than 30 billion records. It is basically a community / eco system that must be managed and coordinated towards the common goal of ensuring that the product / service security is taken care of and in a sustainable manner. In this study the attempt is made to tailor a safety net, if the expected behaviors of responsible disclosure are not followed and any of the barriers explained above turns out as a threat motivating actor, resulting in a publication of identified vulnerability in any non-designated format. For e.g. in any forums, dark net etc. The topics mentioned under barriers can influence the way a disclosure is made. The lack of a global law enforcement also is a lack of control by which an enraged researcher might think of an open disclosure of the vulnerability that he has found out rather than sharing it in the authorized platform & method. The intelligent security response system (ISRS) is envisioned as a vigilant tool which helps the product management companies to put a focus crawl based on the key words associated to its newly released products across the web and darknet. Any detection of key words in the internet or dark net is tracked and filtered according to its relevance and raked. This is supplied as a feed to the PSIRT's which then follows the regular security response practice as mentioned in chart 1. The intelligence ISRS is bringing in is from the module designed to learn the different patterns of search, filtering and raking and influence the way the results are obtained. This makes the system to detect the flaws in a faster way and helps with faster actions.

Breach of an existing protocol which is implemented, is the high level of the problem that is being discussed in this paper. Responsible disclosure is a protocol which is implemented around its own eco system. And this is working for many years. There were no major attempts done on finding the efficiency of this established protocol. i.e. to what extend exceptions are happening. This is a dimension of the issue that we are trying to address in this project as an issue. During the reporting cycle if there is an unexpected behavior which is contrary to responsible disclosure, there are limited resources available now which helps the company to proactively identify the issue and apply corrective measures. The lack of acting on time can create multiple damages to the product company such as breach on customer data, brand damage, financial loss and legal issues. Some of this are long term caused due to cultural & organizational issues while some others relate to the technological and financial topics. While it is easier to tackle the latter issues, former needs more time to identify and correct. Cloud disruptions adds to this complexity as there is a severe lack of comprehensive coverage of the inputs from the good actors (White HAT organizations, Ethical Hackers). Also, sometimes the staggered input mechanisms affect the efficiency of initial triage as there would be a high input volume, or at least during the times when there is a spike with respect to input volume. Since many of the organizations doesn't have embraced fully the shift left approach, there would be often a lack of support from the product development area due to multiple reasons, priority & capacity being the main ones. When there are such challenges it creates business dependencies and adjustments would have to be accommodated as part of operational implementation. When converting this uncertainty into money it helps us understand the impact business is facing. Chart 2 below talks about the amount of monetary damages caused due to cybercrimes from 2001 till 2020. There is for sure a part of this which would have been not identified via the responsible disclosure process. Or in other words, if the responsible disclosures were working perfectly as it was expected to be there would have been a considerable reduction over the period of years. The reason for making such a statement is because the IT spend which is explained in Chart 3 clearly indicates that the investment is increasing year after year. A portion of that budget is going proportionally towards responsible disclosures and still we can see an increasing trend of vulnerabilities.

1.1 Objectives

The ISRS project study aims at addressing the issues of lack of responsible disclosures primarily, along with its attempt to find out efficient ways of trying to predict the zero days attacks. Considering the general scenario of responsible disclosure cycles, despite the increased investment in Cyber Security as a whole, the vulnerabilities are always on an increasing trend. To have a control on the bad actors (Hackers, Grey Hat organisations) is highly unlikely as there is a limit to which governments, and law enforcements can control these. In other words, if the bad actors are not controllable by the existing frameworks, there is always the chance that the product, companies are getting exploited. In today's world of tough competition severe damage to the brand value can cause catastrophic effect on the company. Along with developing capability to handle the relevant data collected by crawling across various web sites, CVE database of MITRE using free API's, the ISRS study was also focused on providing reliable information search related to the key words from the darknet. Some of the deviated disclosures often lands in the darknet and by providing a constant search presence there it is intended to have more details collected and provided to stakeholders so that an ample amount of time is provided for the reaction and damage control. The objective of this study is to provide alternate approaches or solutions that could be used by the impacted parties specific to the identified problems. With the conducted study and simulations, it was very evident that the suggested approaches can be advantageous. Also, it can help organizations to be more effective in terms of addressing the issues reported during the productive usage. The study also aims at providing a future direction of thought, that could improve the current situation, and it also aims at providing a barnstorming on the additional investments needs to protect the business interest. The key differentiator for ISRS is that it allows a focused proactive search methodology within a stipulated time. So, this would ideal to be used together with go lives or cutovers rather than on a generic day to day activity. The crawl and ranking mechanism need enhancement based on the experience of running this solution is live mode. The output generated is filtered and it is expected that in the initial run there could be some false positives which would be improved with the exposures to more patterns and learning.

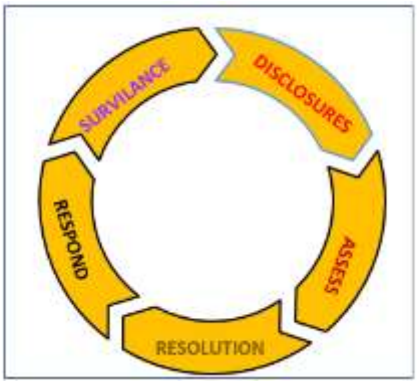

Chart-1 Lifecycle of Product Security Response

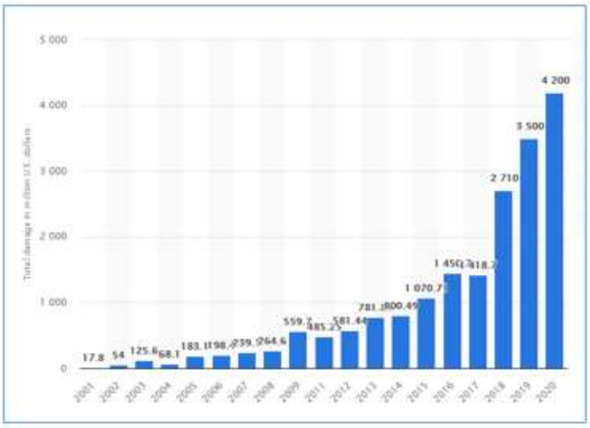

Chart-2 Financial Impact

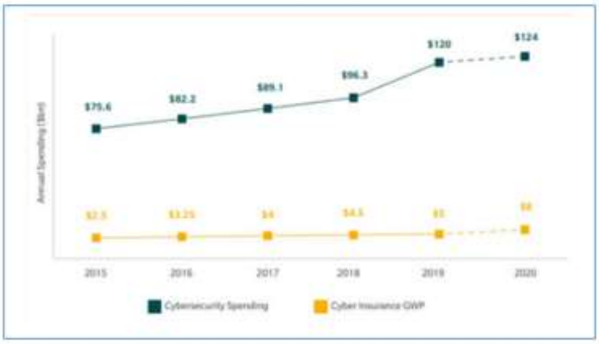

Chart-3 Cybersecurity Spending

2. CONCLUSION

The study was done both from an PSIRT and a customer point of view and hence the inputs are catering to both dimensions. In the entire responsible disclosure chain of actions , this project clearly attempts to signify the importance of the response to the reported vulnerabilities and ensuring that the KPI’s advertised are adhered to so that the chances of a breach in the responsible disclosure is rarely happening. Nevertheless in such cases of breach, ISRS is attempting to catch such behaviors based on the key word search utility within the CVE DB’s and the public and dark nets and the self-learning capability is ensuring that the false positives are kept to the minimum.

3. REFERENCES

[1] T. D. Wagner, &quot;Cyber Threat Intelligence for “Things”,&quot; 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2019, pp. 1-2, doi: 10.1109/CyberSA.2019.8899384

[2] K. Nakao, &quot;Proactive cyber security response by utilizing passive monitoring technologies,&quot; 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, 2018, pp. 1-1, doi: 10.1109/ICCE.2018.8326061.

[3] L. H. Soo, &quot;Comparative analysis of Governmental Countermeasures to cyber attacks,&quot; 2015 International Carnahan Conference on Security Technology (ICCST), Taipei, Taiwan, 2015, pp. 1-6, doi: 10.1109/CCST.2015.7389664.

[4] J. Steinke et al., &quot;Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research,&quot; in IEEE Security &amp; Privacy, vol. 13, no. 4, pp. 20-29, July-Aug. 2015, doi:10.1109/MSP.2015.71.