RESEARCH REVIEW JOURNALS
Volume-05
Issue-07
July-2020

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[Peer Reviewed Journal]
DOI: https://doi.org/10.31305/rrijm.2020.v05.i07.025

A Strategic approach, Issues and Challenges of Adaptive Cyber Security

[1]Dr. Kirit I. Chokhawala, [2]Dr. Vishal H. Bhemwala and [3]Dr. Jayesh N Modi

[1,2,3]*Assistant Professor, Deptartment of Computer Science, Hemchandracharya North Gujarat University, Gujarat (India)*

ARTICLE DETAILS

Article History
Published Online: 25 July 2020

Keywords
Cryptography, Security, Email Security, IP Security, Web Mining, Data and Information Security.

[*]**Corresponding Author**
Email: kiritmca[at]gmail.com

ABSTRACT

Cyber security means protection of valuable computer resources like Hardware, Software, Data and Network. Now a day lots of tools and technology available over the network, it is really impossible for the cyber security to trace threat in real time manner. There are lots of tools which provide protection to the cyber security. Many of them have it own disadvantage of usage. Firewall dependents on the network information available from the router. Intrusion Detection System dependents on the rules set by organization. Even they all works fine prone to be hack. These are software system and software itself is hacked and misused by malicious software (Antivirus). To identify probable threat in real time it is impossible for the cyber security tools to early detect and recover system. Hence, change in technology always demand. Security developer and cracker always "race like Micky and Mouse". The change in security requirement is historical events. I can prove. The Great Wall of China is serving the security need when airplane and other flying object were not discovered. In today, they are ineffective security tools because of many advent tools like missile and submarine has been developed. Same as in the field of cyber security now time comes we need to correct our older security system and one possible solution is adaptive cyber security. Adaptive cyber security is the tools for early warnings to the system. Even attack was not initiated but it is going to give hint based on the system that uses stored data in to the system. Unusual pattern has been analyzed that results in the early indication of unauthorized person or machine tries to steal the information or damage the current security system. It still in its early life, there are so many challenges and issues needs to be concern. In this paper I want highlight the same challenges and issues are going to be face when adaptive cyber security is implemented.

1. Introduction

Adaptive Security is an approach to cyber security that analyzes behaviors and events to protect against and *adapt* to threats before they happen. With an Adaptive Security Architecture, an organization can continuously assess risk and automatically provide proportional enforcement that can be dialed up or down. Organizations today are facing constant security threats from both external and internal sources. They need to be prepared and to maintain a robust set of security policies that can be applied across their enterprise. Due to the constant evolution of security threats, it is no longer enough for organizations simply to use blocking mechanisms or after-the-event procedures to prevent and respond to attacks.

Adaptive Security is a real-time security model or approach that continuously investigates behaviors and events to protect against the threat and adapt to the threats accordingly before they happen. The primary goal of adaptive security is to create a feedback loop of threat visibility, detection, and prevention that consistently becomes more effective. It consists of four major categories of competence, that are – **Prevention, Detection, Responsive, and Prediction.** "**Prevention** is better than cure". Make system so much harder so it is impossible for any threat to get through. Early **Detection** allows us to rollback attack and do very less damage to the system. **Responsive** means system is so alert that it can response in no time and protect system. In future if any such kind of attack is initiated that can be **predictable.**

Many cyber security threats are known in well advanced but few of them may arrive new and hence, quantifying security threat is quite impossible for all most all the cyber security organization. Organizations empower them to predict, prepare and react proactively to the shifting and changing challenge of the cyber security threat. No matter what the size of your network, the nature of your business or the threats you are exposed to, adaptive security is just that - it can adapt to the needs of your business and evolve to ensure you have the policies and procedures in place to protect you from the existing threat landscape. By adopting adaptive security architecture, your organization can get a better understanding of strengths and weaknesses across the environment and access security requirements with greater accuracy. Dynamic Data Protection (DDP) from Force point is one of the easiest and most effective ways to move towards adaptive security architecture. Dynamic Data Protection surfaces anomalies, and proactively adjusts individualized data security controls in near real-time to protect your data.

2. Traditional Security V/S Adaptive Security

Nowadays organizations and security professionals are facing a combination of challenges which include undefined perimeters and continuously evolving security aspects. New problems may consist of the evolution of the IoT and IoE, the transition from IPv4 to IPv6. Due to the emerging of such new trends and most of the previous attacks the market has seen in the past few years, there is one common threat, i.e., the attacker has penetrated the traditional perimeter defenses, which show traditional log event management tools, and monitoring practices are becoming increasingly insufficient, the firewall or IPS monitors the communication between devices and tries to spot an attack in the traffic based on having seen such an attack before, which is not a much of intelligent defenses where attacks are becoming automated and smarter.

It is essential that organizations should shift their security mindset from 'incident response' to 'continuous response' by adapting the Adaptive Security Architecture (ASA).

3. Adaptive Security Architecture (ASA)

Adaptive security architecture describes an approach that uses a combination of integrated tactics to help businesses

stay ahead of cybercriminals, instigating flexible security measures to protect data and systems in as agile a way as possible, rather than relying on outdated perimeter defense strategies.

The Adaptive Security Architecture is the enterprise security immune system. Adaptive Security Architecture (ASA) is based on solutions that use adaptive and dynamic operational styles to maintain the integrity of data, systems and their survivability. To extend the parallel between biological ecosystems and enterprise IT infrastructures, ASA follows the Darwinian concept of 'adapt or die'. Successful IT infrastructures must adapt or they will eventually fall to predator attacks, viral infections or the inability to adjust to environmental changes. ASA behaves similarly to how an organism defends against a localized disease outbreak or even a pandemic. Using an adaptive approach, ASA is an autonomic system that effectively mimics both an organic immune system and a large-scale natural ecosystem. To this end, the key objective of an Adaptive Security Architecture (ASA) is to be able to detect, contain and respond to cyber threats before they cause damage by:

- Continuously monitoring the "entire IT stack"
- Shifting from "incident response" to "continuous response"
- Moving to a "unified" or "integrated" detection, response, prediction & protection capability
- Preventing "successful attacks"
- Reducing the surface and velocity of attacks
- Reducing the Mean-Time-To-Detect Threats (MTTD) and the Mean-Time-To-Respond to Threats (MTTR)
- Implementing a continuous response-enabled operations (SOC) Moreover, the ASA has to provide the ability to take remedial actions such as:
- The quarantine of resources for forensic purposes so that the ecosystem can learn from the breach
- The provisioning of other resources to replace affected systems, enabling service continuity
- The application of corrective measures as needed.

3.1 Components of adaptive Security Architecture

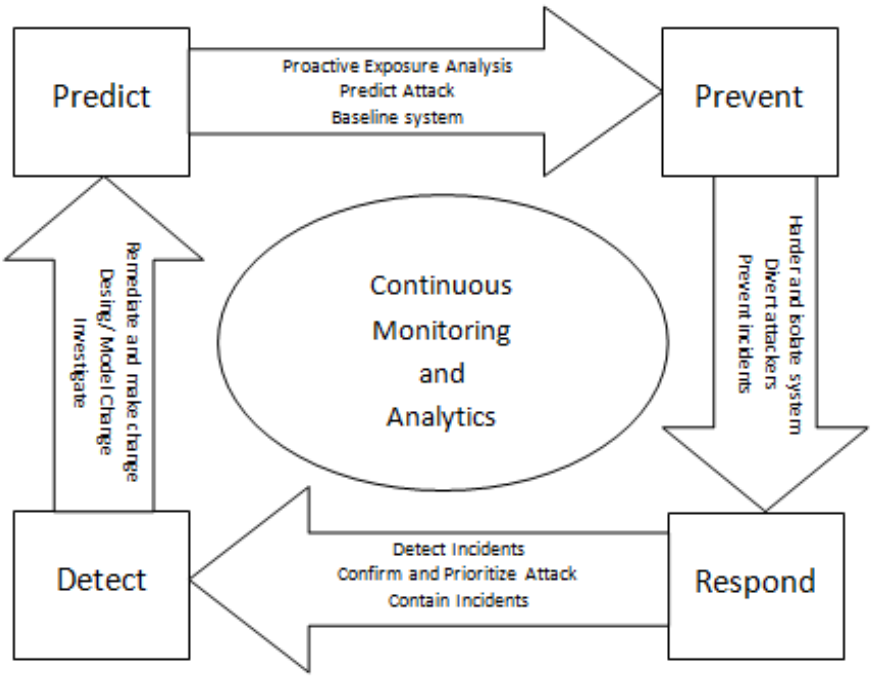
The adaptive security architecture refers to provides continuous, pervasive monitoring and visibility.

- "To enable a truly adaptive and risk-based response to advanced threats, the core of a next-generation security protection process will be continuous, pervasive monitoring and visibility that are constantly analyzed for indications of compromise."
- "Enterprise monitoring should be pervasive and encompass as many layers of the IT stack as possible, including network activity, endpoints, system interactions, application transactions and user activity monitoring."
- "Improved prevention, detection, response and prediction capabilities are all needed to deal with all types of attacks, 'advanced' or not. Furthermore, these should not be viewed as soloed capabilities; rather, they should work intelligently together as an integrated, adaptive system to constitute a complete protection process for advanced threats."

3.2 Stages of Adaptive Security Architecture

There are four stages of adaptive security architecture as: predict, prevent, respond and defect. These can be briefly defined as:

- Predict – assess risk, anticipate attacks and malware, implement baseline systems and posture.
- Prevent – harden and isolate systems to prevent security breaches.
- Respond – investigate incidents, design policy changes, conduct retrospective analysis.
- Defect – prioritize risks, defect and contain incidents.



3.3 Objectives of Adaptive Security Architecture

Following are the objectives of Adaptive Security Architecture:

- Reduce threat amplification – it restricts the potential spread of a pandemic in a monoculture.
- Shrink the attack surface – make the target of an attack smaller
- Decrease attack velocity – slow the rate of attack
- Reduce remediation time – respond to an attack quickly

- Facilitate the availability of data and processing resources – prevent or contain attacks that try to limit resources
- Promote correctness of data and the reliability of processing resources – respond to attacks intended to compromise data or system integrity.

3.4 Benefits of Adaptive Security Architecture

Companies have always relied on prevention and policy-based controls for security, deploying products such as anti-virus software, IDS/IPS and firewalls. Today, we are flooded by advanced and targeted attacks. However, the security architect can advise a shift in the security mindset from 'incident esponse' to 'continuous response', by assuming that systems are compromised and require continuous monitoring and remediation. Adaptive Security Architecture has the potential to provide organizations and businesses with the following benefits.

- Real-time Monitoring and Responses: Teams are enabled to move from after-the-fact analysis logs to real-time evaluation of users. This makes a dynamic, immediate and potentially autonomous response possible.
- Filtering and Prioritizations: By applying advanced analytics and machine learning, organizations can identify some on-going security breaches they cannot detect by monitoring the system alone.
- Reduce Threat Amplification: Restrict the potential spread of a pandemic in a monoculture.
- Shrink the Attack Surface: Make the target of an attack smaller.
- Decrease the Attack Velocity: Slow the rate of attack.
- Reduce Remediation Time: Responds to attack quickly.

3.5 Key Challenges

- Existing blocking and prevention capabilities are insufficient to protect against motivated, advanced attackers.
- Most organizations continue to overly invest in prevention-only strategies.
- Limited visibility in advanced attacks.
- Because enterprise systems are under continuous attack and are continuously compromised, an ad hoc approach to "incident response" is the wrong mindset.

3.6 Recommendations

- Shift from "Incident response" to "Continuous response".
- Adopt an adaptive security architecture.
- Spend less on prevention; invest in detection, response and predictive capabilities.
- Develop a security operations center that supports continuous monitoring.

4. Analytics and Machine Learning in Adaptive Security

A primary tenet of adaptive security is to always assume there is something wrong with the system. Continual monitoring and improvements of security architecture are the main priorities. The modus operandi is to not wait for an incident to happen, but to expect it, identify it, and respond before having the chance to breach the system. It needs to be a proactive approach model as opposed to a reactive one. Security analytics and machine learning are key components of adaptive security architecture. In addition to this, descriptive analytics detect anomalous events, diagnostic analytics help explain why an adverse event happened and predictive analytics can identify suspicious behavior based on historical data and patterns – both on microscopic and macroscopic levels. With endless reams of Big Data locked up in data warehouses in the cloud and malicious activity disguised as legitimate commands, and server requests becoming nearly impossible to detect, machine learning can serve a useful purpose.

It can assist a security team by automating many processes such as pattern recognition used in analytics. Machine learning is used to review data from tens of millions of data logs per day. It reduces the number of events a cyber security analyst must review from one or two hundred to tens of thousands. With the ability to autonomously learn from past successes and failures, it has an 85% success rate predicting cyber attacks.

5. Conclusion

In this paper, Adaptive Cyber Security Techniques with its architecture, benefits and challenges were discussed. It is clearly stated that because of unpredictable behaviors of cyber attack, there must be need to develop a new way of security mechanism. The word has seen a promising development in the Adaptive cyber security which meets the changing and futuristic requirements of security. It has shown various challenges has been found but the integrating approach with existing technology and analytical tools it is going to defiantly found solution.

References

[1]. *"Gartner Details Real-Time 'Adaptive' Security Infrastructure". Retrieved 6 January 2009.*
[2]. *"Special Webcast: Real-Time Adaptive Security: Proactively Mitigating Risks". Retrieved 6 January 2009.*
[3]. A Cybersecurity Agenda for the 45th President. (2017, January 5). Retrieved from https://www.csis.org/news/cybersecurity-agenda-45th-president
[4]. An Examination of the Cybersecurity Labor Market. (n.d.). Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf
[5]. Applications Now Available for City Colleges of Chicago's New Cyber Security "Boot Camp". (2017, March 18). Retrieved from http://www.ccc.edu/news/Pages/Applications-Now-Available-for-City-Colleges-of-Chicagos-New-Cyber-Security-Boot-Camp-.aspx
[6]. ApprenticeshipUSA Investments. (2017, June 22). Retrieved from https://www.dol.gov/featured/apprenticeship/grants
[7]. Assante, M., Tobey, D. (2011, February 4). Enhancing the Cybersecurity Workforce. Retrieved from http://ieeexplore.ieee.org/document/5708280/
[8]. Assessment Act. Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/2007/text
[9]. ATE Centers. (n.d.). Retrieved from http://www.atecenters.org/
[10]. ATE Centers and National Science Foundation. (n.d.). ATE Centers Impact Report. Retrieved from http://www.atecenters.org/wp-content/uploads/PDF/ATEIMPACT_2016-17.pdf
[11]. ATE Centers and National Science Foundation. (n.d.). ATE Programs and Overview. Retrieved from http://www.atecenters.org/wp-content/uploads/2016/07/ATE_Overview_2016.pdf

[12]. AUSTRALIA'S CYBER SECURITY STRATEGY Enabling innovation, growth & prosperity [PDF]. (n.d.). Retrieved from https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
[13]. Baltimore Cyber Range and Cyberbit Open New Cybersecurity Training and Simulation Center. (2017, August 3). Retrieved from https://www.cyberbit.com
[14]. Bessen, J. (2014, August 25). Employers Aren't Just Whining – the "Skills Gap" is Real. Harvard Business Review. Retrieved from https://hbr.org/2014/08/employers-arent-just-whining-the-skills-gap-is-real
[15]. Best in Class Strategies for Entry-Level Employee Retention Prepared for 100K [PDF]. (2016, October). FSG Reimagining Social Change. Retrieved from https://www.100kopportunities.org/2016/10/14/best-in-class-strategies-for-entry-level-employee-retention/
[16]. Best Places to Work for Cyber Ninjas. (2017, May). Retrieved from https://www.sans.org/best-places-to-work-for-cyber-ninjas?ref=195285
[17]. Bojanova, I., Vaulx, F., Zettsu, K., Simmon, E., Sowe, S. (2016, January 21). Cyber-Physical-Human Systems Putting People in the Loop. IT Professional. Retrieved from http://ieeexplore.ieee.org/document/7389271/
[18]. Burning Glass Technologies. (2015). Job Market Intelligence: Cybersecurity Jobs, 2015 [PDF]. Retrieved from http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
[19]. Canadian Apprenticeship Forum Forum Canadien Sur l'Apprentissage. (2009, June). It Pays to Hire an Apprentice: Calculating the Return on Training Investment for Skilled Trades Employers in Canada A Study of 16 Trades Phase II Final Report. Retrieved from http://www.wi-cwi.org/council/2014/morgan_apprenticeship_canada_roi_011514.pdf
[20]. Carlini, J. (2017, August 6). Geneva Convention in Cyberwarfare? Don't Count on It. Retrieved from

