International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi :https://doi.org/10.32628/IJSRST218670

Cyber Security : Techniques and Perspectives on Transforming - A Review

Shruti Sunil Ajankar*, Aditi Rajesh Nimodiya
B.E, Department of C.S.E, Jawaharlal Darda Institute of Engineering and Technology, Yavatmal, Maharashtra, India

Article Info
Volume8, Issue 6
Page Number:473-480

Publication Issue
November-December-2021

Article History
Accepted :15 Dec 2021
Published :30 Dec 2021

ABSTRACT

Cyber Security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. So basically it is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risks of cyber attacks and protect against the unauthorized exploitation of systems, networks and technologies. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on some of the techniques and perspectives on transforming the cyber security.Here we have discussed a new posture for cyber security in a networked world which explains how companies can use organizational structure and governance to enhance cybersecurity protections.

Keywords: Cyber attacks, Cyber crimes, Techniques, Cyber security, Transforming, Perspectives

I. INTRODUCTION

Cyber Security is the technique to protect our data from unauthorized access or malicious attack.

We can divide cyber security into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information.[3]

It wasn't too long ago that sophisticated executives could have long, thoughtful discussions on technology strategy without even mentioning

security. Today, companies have substantial assets and value manifested in digital form and they are deeply connected to global technology networks – even as cyber attackers become even more sophisticated and adaptable to defences. At most companies, boards and senior executives acknowledge the serious threats that cyber attacks pose to their business. What they are not sure of is how to create a strategy that helps them understand and address the threats, in all their forms, today and in the years ahead.

The fight against cyber crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes.

cyber attacks pose to their business. What they are not sure of is how to create a strategy that helps them understand and address the threats, in all their forms, today and in the years ahead.

II. TECHNIQUES

1)Maintain an Accurate Inventory of Control System Devices and Eliminate Any Exposure of this Equipment to External Networks

Never allow any machine on the control network to talk directly to a machine on the business network or on the Internet. Although some organizations' industrial control systems may not directly face the Internet, a connection still exists if those systems are connected to a part of the network – such as the corporate side – that has a communications channel to external (nontrusted) resources (i.e., to the Internet).

Organizations may not realize this connection exists, but a persistent cyber threat actor can find such pathways and use them to access and exploit industrial control systems to attempt to create a physical consequence. Therefore, organizations are encouraged to conduct thorough assessments of their systems, including the corporate enterprise segments, to determine where pathways exist. Any channels between devices on the control system and equipment on other networks should be eliminated to reduce network vulnerabilities.

- ICS-ALERT-12-046-01AIncreasing ThreattoIndustrialControlSystems(ICS-CERT)
- ICS-ALERT-11-343-01AControlSystemInternetAccessibility(ICS-CERT)
- Targeted Cyber Intrusion Detection and Mitigation Strategies(ICS-CERT)

2)Implement Network Segmentation and Apply Firewalls

Network segmentation entails classifying and categorizing IT assets, data, and personnel into specific groups, and then restricting access to these groups. By placing resources into different areas of a network, a compromise of one device or sector cannot translate into the exploitation of the entire system. Otherwise, cyber threat actors would be able to exploit any vulnerability within an organization's system – the "weakest chain in the link" – to gain entry and move laterally throughout a network and access sensitive equipment and data. Given the rise of the "Internet of Things" – whereby many previously non-Internet connected devices, such as video cameras, are now linked to systems and the web – the importance of segmenting networks is greater than ever.

Access to network areas can be restricted by isolating them entirely from one another, which is optimal in the case of industrial control systems , or by

implementing firewalls. A firewall is a software program or hardware device that filters the inbound and outbound traffic between different parts of a network or between a network and the Internet. For connections that face the Internet, a firewall can be set up to filter incoming and outgoing information. By reducing the number of pathways into and within your networks and by implementing security protocols on the pathways that do exist, it is much more difficult for a threat to enter your system and gain access to other areas .Creating network boundaries and segments empowers an organization to enforce both detective and protective controls within its infrastructure. The capability to monitor, restrict, and govern communication flows yields to a practical capability to baseline network traffic (especially traffic traversing a network boundary), and identify anomalous or suspicious communication flows.

3)Use Secure Remote Access Methods

The ability to remotely connect to a network has added a great deal of convenience for end users, but a secure access method, such as a Virtual Private Network (VPN), should be used if remote access is required. A VPN is an encrypted data channel for securely sending and receiving data via public IT infrastructure (such as the Internet). Through a VPN, users are able to remotely access internal resources like files, printers, databases, or websites as if directly connected to the network. This remote access can further be hardened by reducing the number of Internet Protocol (IP) addresses that can access it by utilizing network devices and/or firewalls to specific IP addresses and/or ranges and from within the U.S. Note that a VPN is only as secure as the devices connected to it. A laptop computer infected with malware can introduce those vulnerabilities into the network, leading to additional infections and negating the security of the VPN.

4)Establish Role-Based Access Controls and Implement System Logging

Role-based access control grants or denies access to network resources based on job functions. This limits the ability of individual users – or attackers – to reach files or parts of the system they shouldn't access. For example, SCADA system operators likely do not need access to the billing department or certain administrative files. Therefore, define the permissions based on the level of access each job function needs to perform its duties, and work with human resources to implement standard operating procedures to remove network access of former employees and contractors. In addition, limiting employee permissions through role-based access controls can facilitate tracking network intrusions or suspicious activities during an audit.

5)Use Only Strong Passwords, Change Default Passwords, and Consider Other Access Controls

Use strong passwords to keep your systems and information secure, and have different passwords for different accounts. Hackers can use readily available software tools to try millions of character combinations to attempt an unauthorized login – this is called a "brute force attack." Passwords should have at least eight characters, but longer passwords are stronger, because of the greater number of characters to guess. Also, include uppercase and lowercase letters, numerals, and special characters. Change all default passwords upon installation of new software, particularly for administrator accounts and control system devices, and regularly thereafter. Implement other password security features, such as an account lock-out that activates when too many incorrect passwords have been entered. Organizations may also consider requiring multi-factor authentication, which entails users verifying their identities – via codes sent to devices they previously registered – whenever they attempt to sign-in.

6)Develop and Enforce Policies on Mobile Devices

The proliferation of laptops, tablets, smartphones, and other mobile devices in the workplace presents significant security challenges. The mobile nature of these devices means they are potentially exposed to external, compromised applications and networks and malicious actors. Further contributing to this challenge is the increasing trend of organizations allowing employees to use their personal electronic devices for work purposes, known as the "Bring Your Own Device (BYOD)" phenomenon.

Therefore, it's important to develop policies on the reasonable limits of mobile devices in your office and on your networks. These measures should be strictly enforced for all employees, as well as for contractors. Devices should also be password protected to ensure only authorized users can log-in. Otherwise, an unauthorized user can gain access to restricted networks and files using an authorized user's device. Similarly, employees should avoid or be cautious about using devices that do not belong to them as they cannot be sure these are properly protected or comply with established policy. Such devices may actually be infected, and using them could put the information and networks you access at risk.

III. WHY CURRENT SOLUTIONS FALL SHORT

To combat the risks of malicious insiders, most companies rely on user-behavior monitoring software.

These rules-based or machine-learning based applications ingest troves of data about employee actions, especially their use of IT systems. Generally, they attempt to identify divergence from what is considered "normal" behavior for that employee. When the software spots an anomaly, a small team investigates.

While this method can be helpful, we find that it usually falls short, for four reasons:

-By the time negative behaviors are detected,the breach has often already occurred. Theorganization is already at a disadvantage, and itcannot deploy an active defense.

-Monitoring for "divergence from normal behavior" creates a huge number of false positives, wasting much of the investigation team's time.

-Serial bad actors may not be caught; malicious activity may be built into the baseline of "normal" activity.

-Collecting massive amounts of employee datacreates privacy concerns and significant potential for abuse.

Beyond these issues, some organizations take this type of monitoring to an extreme, deploying military grade software and conducting full-blown intelligence operations against their employees. Several recent news stories have highlighted the risks of overstepping the organization's cultural and privacy norms. Best practices and necessary precautions in the defense industry may be seen as invasive at a bank or insurer. Finally, to the extent that companies pursue insider threat, they often focus on malicious actors. While most cyber organizations know that negligence is an issue, many start and end their prevention efforts with half-hearted employee education and anti-phishing campaigns.

IV. A BETTER WAY

Some leading cybersecurity teams are using a differentapproach, built on three pillars:

Microsegmentationallows the organizationto home in on the "hot spots" of risk and take a targeted rather than blanket approach to threatmonitoring and mitigation.

Culture changemakes malicious, co-opted, ornegligent risk events less likely, and puts thecompany in a preventive rather than reactiveposture.

Predictionallows an organization to identifyand disrupt insider activities much earlier in thethreat life cycle.

Microsegmentation

Rather than going immediately to wholesale monitoring, we believe that organizations should take a much more nuanced approach, tailored to their information assets, potential risk impacts, and workforce. The key to this approach is microsegmentation, which identifies particular groups of employees that are capable of doing the most damage, and then develops focused interventions specific to those groups.To create a microsegmentation, the first step is to understand the business capabilities or information most important to protect. Next, companies can use identity-and-access-management (IAM) records, as well as organizational and HR information, to determine which groups and individual employees have access to those assets. These groups form the microsegments that are most important for the program to focus on. For each segment, a company can then determine which types of insider threats are most likely to cause damage, and it can create differentiated strategies to monitor and mitigate insider events. Imagine that a pharmaceutical company wants to protect the intellectual property created in new drug development. An analysis of IAM and HR data reveals that specific portions of its product-development and its R&D organizations represent the highest risk. The company knows that sabotage of this kind of IP is relatively rare (other researchers would easily catch mistakes), but that flight risks—scientists who take IP with them when hired by competitors—are very probable. The company designs strategies to identify flight risks in the R&D team (such as people who missed promotions, poor workforce satisfaction, and low pay relative to peers), and then monitors the group for these characteristics. The company could then design interventions, such as retention programs, specially for its flight risks. Microsegmentation offers three key benefits. First, it creates a clearer understanding of risk; not all insiderthreat events are created equal. Second, it allows organizations to identify a clear set of remediation actions, tailored to a particular group of employees.

This helps them to move from reacting to insiderthreatevents to preventing them. Finally, the analysisallows the organization to monitor groups ratherthan individuals, using metrics such as employeeattrition and workforce satisfaction of a team ratherthan individual behaviors. This provides significantprivacy benefits.

Culture change

While many programs focus on catching and responding to negative behaviors, it's also vitally important to directly and assertively address the cultural issues that drive negligence and malicious behavior. To combat negligence and co-opting, companies often conduct rudimentary cybersecurity trainings, as well as phishing testing. Too often these focus only on behavior—educating employees on proper cyberprocedure and miss the attitudes-and-beliefs part of the equation. Targeted interventions (such as periodic communications on cyber-impact) help employees see and feel the importance of "cyber-hygiene," and purposeful reinforcement from senior executives iscritical to achieving workforce buy-in. Best-in-classorganizations rigorously measure both behaviors andattitudes and develop comprehensive change plans tobeat cyber-negligence, complete with targets and clearowners within the organization. Addressing the drivers of malicious behavior is an even more personal task. The drivers vary for each

organization, and often for each microsegment. For instance, they might include personal financial stress, disgruntlement over lack of promotion, or flight risk due to poor management. Organizations that successfully address drivers of malicious behavior often begin by analyzing workforce trends (using satisfaction surveys, for example) to determine potential hot spots. They then design changes in process, governance, hiring, compensation, and so on, specific to the identified risk areas aligned to their microsegmentation strategy. For example, if an employee group has a high prevalence of "flight risks" due to disgruntlement over a manager, the organization may require leadership coaching or even rotating the manager out of the group. If financial stress seems to be an issue, the organization may choose to provide free financial-planning help or to reevaluate its compensation model.

Prediction

Advanced organizations are taking one further step to identify groups or individuals early in the threat life cycle: predictive insider-persona analytics. The and have been studied at length. High – performingorganizations have identified the markers of thesepersonas and actively monitor these markers formain personas that present a risk are well establishedspecific personas, rather than looking for divergencefrom normal. This analysis can identify a group orindividual likely to represent a threat well before theevent takes place; companies can then take steps tomitigate the threat.

A NEW POSTURE

To ready global companies for an age of all-encompassing connectivity, executives need a more adaptive, more thorough, and more collaborative approach to cyberrisk . We have observed the followingprinciples used by some of the world's leading cybersecurity teams at global companies:

Cyberrisk needs to be treated asa risk management issue not an IT problem

Cyberrisk is much like any other complex, critical, nonfinancial risk. Key elements of its management include the prioritization of relevant threats, the determination of a company's risk appetite (its willingness to accept some risk), and the definition of initiatives to minimize risk. Additionally, companies need to put in place an organizational structure and a governance approach that bring transparency and enable realtime risk management.

Companies must address cyberrisk in a business context

Technical experts cannot solve the problem without understanding the underlying commercial and organizational requirements. Companies tend to overinvest in technical gadgets and underinvest in complexity reduction and consistent coverage of their whole value chain, such as vendor risk management. The result is an inefficient system.

Companies must seek out and mitigate cyberrisk on many levels

Data, infrastructure, applications, and people are exposed to different threat types and levels. Creating a comprehensive register of all these assets is tedious and time consuming .Companies should take advantage of
automated tools to catalog their assets, the better to focus on those at most risk.

Adaptation is essential

sooner or later, every organization will be affected by a cyberattack. A company's organization, processes, IT, OT, and products need to be reviewed and adjusted as
cyberthreats evolve. In particular, companies must fine-tune business - continuity and crisis management structures and processes to meet changes in the threat level.

Cyberrisk calls for comprehensive,collaborative governance

Traditionally, many companies distinguish between physical and information security, between IT and OT, between business-continuity management and data protection, and between in-house and external security. In the digital age, these splits are obsolete. Scattered responsibility can put the entire organization at risk. To reduce redundancies, speed up responses, and boost overall resilience, companies need to address all parts of the business affected by cyber threats— which is to say, all parts of the business, and suppliers and customers too. While it may be hard—or even impossible—to protect a companyagainst the most advanced attacks, systematicgovernance is the best insurance against the bulkof everyday attacks.

Companies that adhere to these principles tend to be much more resilient to most attacks than their peers.A defense ministry set out to ramp up cyberresilience across its entire organization. Scenario exercises helped increase cyberrisk awareness and instill a sense of urgency, by focusing on the mind-set of potential attackers and the concept of the weakest link in the chain of defense. Through an extensive training program, this kind of thinking was rolled out to the entire agency, making sure skills were passed on from expert to expert. Throughout, the intelligence unit acted as the stronghold of cybersecurity expertise and the catalyst of change. In parallel, the institution reviewed and adjusted its IT architecture to increase resilience against destructive attacks, such as those that corrupt current data and backups, leading to a nonrecoverable situation. The new approach also makes better use of cybersecurity resources and funds. Just refocusing investment on truly crucial assets can save up to 20 percent of cybersecurity cost. In our experience, up to 50 percent of a company's systems are not critical from a cybersecurity perspective. We've also seen that the cost of implementing a given security solution can vary by a factor of five between comparable companies.

V. CONCLUSION

1. Cyber security is becoming more and more important as world is highly interconnected with different networks.[2]
2. The goal of a cyber security is management program is to identify the risks, understand their likelihood and impact on the business, and then put in place security controls that mitigate the risks to a level acceptable to the organization.[3]
3. Insider threat is one of the largest problems in cybersecurity, representing a massive share of attacks and financial damages. Monitoring technologies have their place in organizations'cyber-arsenal. But their effectiveness increases significantly when combined with more nuanced approaches, like microsegmentation, prediction, and direct cultural engagement.[6]
4. Organizations in sectors with higher digital maturity will benefit the most from this approach, including financial services, manufacturing, and healthcare.They face the tough task of fully protecting their most important assets, while not stifling business innovation. To achieve this balance, the business, IT, risk, and other functions will have to work together toward the same, enterprise-wide end—to secure the crown jewels so that the senior leaders can confidently focus on innovation and growth.

VI. REFERENCES

[1] Cyber Security Strategy Of the United Kingdom, safety, security and resilience in cyber space", June 2009. 13-32.

[2] "Why Cyber Security Is Important", State of Wyoming, Office Of the Chief Information Officer, 2001 Capitol Ave, Rm 237, Cheyenne, WY 82002, 2-2.

[3] G.Nikhita Reddy [1]. G.J. Ugander Reddy[2]. "A study of cyber security challenges and its emergning trends on latest technologies", 1-6.

[4] Cyber Security: Strategy to Security Challenges- A Review by Vaishnavi J. Deshpande, Dr. RajeshkumarSambhe in International Journal Of Engineering and Innovative Technology (IJEIT).

[5] Cyber Security Challenges and its Emerging Trends on Latest Technologies by Dr.Prof.Rajasekharaiah K.M, Chhaya S Dule, Sudarshan E in IOP Conference Series: Materials Science and Engineering.

[6] “Perspectives on transforming cybersecurity” , Digital McKinsey and Global Risk Practice March 2019 , McKinsey & Company.

[7] Dr Gulshan Rai, "National Cyber Security Policy", draft volume 1.0, 6-21, 26 Mar 2011.

[8] Cristin Flynn Goodwinl. J. Paul Nicholas2," Developing a National Strategy for Cybersecurity foundations for security, growth, and innovation", October 2013.

[9] Edward Connors. 'CPIanning And Managing Security for Major Special Events: Guidelines for Law Enforcement", March 2007 , 30-128.

[10] 10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks, WaterISAC , October 2016

[11] Prof. Chris Johnson, "Trends in Information Security. Topic Description: The Economics of Threat Analysis for Cyber Security", 3-4.

[12] Introduction to Cyber Security & Cyber Threats- A Review by Aditi Rajesh Nimodiya , Shruti Sunil Ajankar in International Multidisciplinary E-Conference on Contribution of Various Aspects In Nation Building In Association with IJSRST.

Cite this article as :

Shruti Sunil Ajankar, Aditi Rajesh Nimodiya, "Cyber Security : Techniques and Perspectives on Transforming - A Review", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 6, pp. 473-480, November-December 2021. Available at doi : https://doi.org/10.32628/IJSRST218670
Journal URL : https://ijsrst.com/IJSRST218670