Unit 11: Future Trends, Technologies and Challenges for the Information Security Industry

Objectives:

- Review existing and emerging trends and technologies such as SDN and FIAs.
- Discuss some of the security challenges they are designed to overcome.
- Describe the associated issues with new technologies.

Outcomes:

- Describe emerging trends and technologies.
- Explain the impact of emerging changes.
- Describe some challenges encountered with both current and new solutions.

Reflection:

Trends

1. Rise of Automotive Hacking

There are now a wide range of smart processes in today's vehicles that allow users to handle anything from speed control to motor speed to car locks to airbags with the touch of their fingertips. Wireless technologies used in these automobiles expose it to a variety of threats and risks. Automated cars are predicted to lead to an increase in intruding and car control in 2022. A far more complicated approach is required for self-driving or automated cars, which require strong cybersecurity precautions.

2. Potential of Artificial Intelligence (AI.)

As Intelligence has made its way into a wide range of products and services, it has had a significant impact on cyber defense. Autonomous security measures, nlp, facial identification, and autonomous attack detection have all relied heavily on AI technology. Intelligent spyware and assaults that can circumvent the most advanced security measures are also being developed using this technology. AI-enabled risk detection methods can forecast novel assaults and inform administrators of any hacking incident immediately.

3. Mobile is the New Target

There is a 50% rise in digital payment virus or assaults this year, putting the smartphones and tablets a security threat. There are more vulnerabilities to people in all of our images, banking transactions, e - mails, and communications. In 2022, infections and viruses on smartphones could be the focus of internet security concerns.

4. Cloud is Also Potentially Vulnerable

And as more companies go to the clouds, it's essential that safety protocols be continually reviewed and improved in order to prevent data breaches. Regardless of the fact that cloud programmers like Google or Microsoft are very well with privacy from their side, the client side remains a key cause of incorrect mistakes and harmful malware.

5. Data Breaches: Prime target

Agencies around the world will remain focused on data. Irrespective whether you're an individual or a business, protecting your digital data is the most important priority right now. Cybercriminals can gain access to confidential data by any little fault or defect in your web or application. Stricter new guidelines Individuals in the European Union are now protected by GDPR, effected on May 25, 2018. (EU). To protect Californians' privacy rights, the CCPA went into effect on January 1st, 2020.

IoT with 5G Network: The New Era of Technology and Risks

IoT will create a new generation of interconnectedness with the arrival and expansion of 5G technology. There is a risk coming from external interference, assaults, or a computer flaw because of this interconnectedness (Vaezi et al., 2022). Even Google's greatest popular browser, Chrome, was revealed to have severe flaws in its code. As a new technology, 5G technology takes a lot of work to uncover security weaknesses that can be exploited by outsiders. 5G networks may introduce a slew of network threats that we may not be able to detect at a time. To stop data leaks, producers must adhere to extremely tight standards when developing advanced 5G hardware and software.

Challenges:

The propagation of errors

Misconfiguration, which may be the most attractive of all networking security concerns, is nonetheless a major problem. The vast majority of proxy intrusions will be triggered by configuration errors instead of security weaknesses, as per Gartner. The fact that such a basic issue puts companies at danger time after time is really upsetting.

Since networks are becoming increasingly complex, it is becoming increasingly difficult to keep tabs on firewalls. The majority of participants to our State of the Firewall research stated that their firms use more than 100 proxy servers, and 12 percent have over 500. If you're dealing with a lot of things and a lot of rules, it's impossible to do all of this properly. To survive, automation is a need.

However, this does not infer complete automation, the finest way out offers adaptive regulator and distinguishability over systems and proxy servers. In order to reduce human

mistake instead of replace workers, assessment operations during triage and escalation require an awareness of nuance that no machine can provide.

Lack control of privileged access

It is much easy for an attacker to take advantage of preexisting passwords than it is to break into a system, which is why they prefer to misuse privileged access. As a consequence, 74% of assaults are the result of abused privileged access.

Allowing accessibility is a common goal of proxy administration in many businesses. A significant number of users are typically given unnecessarily high privileges as a consequence... This is a risky move on my part. It is necessary to give equal weight to threat and access when evaluating the proxy server as a network security device.

Credentials by themselves do not reveal enough about legitimacy of the person seeking permission. Many additional criteria, such as a person's geography and IP address, must be taken into consideration when determining their identity. IP addresses and geolocations are likely to be unusual as a consequence of COVID-19 work-from-home restrictions. People who return to work in the following months will have to deal with the old status quo.

By eliminating inadvertent mistakes that lead to misconfigurations and enhancing security agility, automation plays an important part in limiting access control misuse. This is incredibly significant throughout extraordinary circumstances like those created by COVID-19. Reducing security misconfigurations is made easier by removing human mistake that can compromise a network that is widely used by distant employees.

Tool interoperability shortcomings

Quite so many tools aren't the issue. The issue is that there are an excessive number of technologies that do not smoothly exchange data.

You can't think of a network as one single area. Micro segmentation and networking regulations and resources produce additional effect in this system of software-defined networks. Security professionals must switch from console to console in order to describe of what each measure signifies in relation to others in attempt to comprehend what's going on in the network. As a result, the situation is ripe for human error and vulnerability.

Since their SIEM is integrated, some firms believe they are protected although if the tools aren't. As a result, SIEMs may miss assaults carried out manually and abnormalities related to a single user, such as a company's marketing employee accessing into a

financial department system without authorization. Traditional security information and event management (SIEM) systems are difficult to use, do not deliver actionable insights, and generate too much data for IT workers to examine.

Technologies for security analysis make data more widely available, allowing for its effective consumption and analysis by a wider audience. The requirement to know a query language is eliminated by natural-language search and analytics. Prerequisite knowledge for integrating data from diverse sources is eliminated because the data gathering will not really involve parsing. Using a security analytics platform, it is possible to identify suspicious activities on a network more quickly.

Lack of visibility

When a new device or endpoint joins or leaves a connection, its exposure constantly changes. Most of the time, it's impossible to know whether or not a connection is protected or compliant. At the very least it's possible for security specialists to reflect back at previous analysis to find whether or not it was safe in the earlier. That isn't knowledge that can be put to use.

There must be a clear understanding of how and why proxy rules are set up, what the ramifications are if they are changed, and how the changes will affect security and compliance. Few businesses are able to accomplish this goal due to the prevalence of recurring issues such as an insufficient availability of IT people, poor network management tools, a lack of knowledge into app distribution routes, and the absence of IT in remote areas. These are just a few. Using automation, it is possible to keep track of, map out, and make adjustments to a system at any particular time. When a member of the SOC has this level of visibility, it has an effect well beyond the SOC. The ability to make changes more quickly and securely while still complying with regulations is one way that visibility benefits the company as a whole. Manage network security risks while also opening up new commercial prospects that provide your company a competitive edge is now possible.

Controls that are out of step with infrastructure changes

Few businesses are able to accomplish this goal due to the prevalence of recurring issues such as an insufficient availability of IT people, poor network management tools, a lack of knowledge into app distribution routes, and the absence of IT in remote areas. Orchestration is the best way to deal with it when dealing with such a large and diverse workload.

Contrary to popular belief, orchestrating is not identical to automating. In contrast to automated processes, orchestration focuses on arranging tasks to perform best inside a process, such as pulling together the entire body of security protocols and automating modification.

Network security must be automated from policy creation to execution in an orchestration solution. It should be able to take pictures of a platform's security posture instantaneously from a live data stream. To ensure scalability, the system should gather and normalize device regulations and security details. Security restrictions and network visibility should be managed from a single, centralized panel.

References

Tabrizchi, H. and Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*. doi:10.1007/s11227-020-03213-1.

Vaezi, M., Azari, A., Khosravirad, S.R., Shirvanimoghaddam, M., Azari, M.M., Chasaki, D. and Popovski, P. (2022). Cellular, Wide-Area, and Non-Terrestrial IoT: A Survey on 5G Advances and the Road Towards 6G. *IEEE Communications Surveys & Tutorials*, pp.1–1. doi:10.1109/comst.2022.3151028.

Zahid, M., Inayat, I., Daneva, M. and Mehmood, Z. (2019). A security risk mitigation framework for cyber physical systems. *Journal of Software: Evolution and Process*, 32(2). doi:10.1002/smr.2219.