Proceedings of National Conference on Multidisciplinary Engineering Sciences and Information technology (NCMESIT, 2020) in Marudhar Engineering College on the 23rd & 24th of November 2020
World Journal of Research and Review (WJRR)
ISSN: 2455-3956, Special Issue, November 2020 Pages 12-14

Enhancement in Security against Digital Attacks

I. B. Singh Sekhawat, Ritesh Kumar Upadhyay, Tushar Barnoliya, Shanendra Singh Nathawat, Premchand Saini

***Abstract*- Security plays a vital role in one's life. For maintaining one's data secure and private, having high security is necessary. Basically, in this changing world cyber-crimes / attacks a person is very insecure. So, to make a person secure some preventive measures are required. This paper is purely based on securing one's details and data i.e., how to enhance the security for one's identity.**
***Index Terms*- Authentication Security, VLANS**

I. INTRODUCTION

Authentication system:
For better and safer functionality for an organization I would use multi-level and multi-factor authentication.
Conceptually, authentication (and SSO) is simple, but it's hard and costly to implement correctly. Though businesses have traditionally focused on building features, now in reality they also must focus on lowering user registration contention without exposing the application to vulnerabilities. Just like how cloud infrastructure platforms (like AWS) now allow businesses to focusing on building apps, we see the same happing with authentication.

I. ***Biometric Authentication:*** Biometric authentication methods include retina, iris, fingerprint and finger vein scans, facial and voice recognition, and hand or even earlobe geometry. The latest phones are adding hardware support for biometrics, such as TouchID on the iPhone. Biometric factors may demand an explicit operation by the user (e.g., scanning a fingerprint), or they may be implicit (e.g., analyzing the user's voice as they interact with the help desk).

I. B. Singh Sekhawat, Assistant Professor, Mechanical Engineering Department, Vivekananda Institute of Technology, Jaipur,
Ritesh Kumar Upadhyay, Mechanical Engineering Department, Vivekananda Institute of Technology Jaipur
Tushar Barnoliya, Student, Mechanical Engineering Department, Vivekananda Institute of Technology Jaipur
Shanendra Singh Nathawat, Student, Mechanical Engineering Department, Vivekananda Institute of Technology Jaipur,
Premchand Saini, Student, Mechanical Engineering Department, Vivekananda Institute of Technology Jaipur

II. ***Password Login Systems with 2-factor authentication:*** As we all know that passwords play an important role in securing important and sensitive information about the user or employee. Besides this we have a 2-factor authentication which will directly help us in securing personal information safer. Here in this work, we implemented these two ways for authentication systems.

External website security:
Any website is built to share information or any kind of data to either facilitate or disturb user whosoever is opening the specific websites. Especially external website are more prone to spread malware or any malicious software. Their aim is to create terror in the minds of people and degrades the reputation of other websites and website hosting platforms. As of this, recommend activating windows firewall and windows defender for prevention from the malicious software and infected website. Except these two no other software is needed for protection from external infected websites.

Internal websites security:
For security of website, it should be updated in regular intervals or frequently so that it should remain safer to use. If in case internal website get infected then don't worry or don't panic. WINDOWS FIREWALL AND WINDOWS DEFENDER will detect it and will block if any malicious software or any hazardous script is trying to get downloaded to your system.

II. REMOTE ACCESS SOLUTION:

Focus on corporate assets, not devices:
As I noted, endpoint device independence (or lack thereof) can play a huge role in facilitating (or inhibiting) remote access. But enabling access from a broad range of devices does not mean ignoring device type or security posture. To that end, many remote access VPNs can now detect endpoint device characteristics, assess risks, and install required security programs or settings -- often without IT or user assistance.
However, these "look before you leap" VPN best practices can still be limited by device type and ownership. Smartphones and tablets may never support the same deep checks that laptops and netbooks do; users may have reasonable expectations of privacy on non-corporate-owned devices.

To avoid circling this drain, consider refocusing security policies on protecting corporate assets instead of the devices

used to reach them. For example, virtual desktop infrastructure (VDI) alternatives (e.g., Citrix XenDesktop, VMware View, and RingCubevDesk) can completely insulate the work environment from the endpoint device by leaving that environment inside the data centre.

III. FIREWALL AND BASIC RULES RECOMMENDATIONSFIREWALL:

It is a virtual wall that detects and blocks all the malicious scripts, applications, software. It is the best way to protect any system from all malicious things that can be downloaded from any network. It also block malware that can be inserted through USB . If we are trying some kind of exploits on our system them firewall and windows defender detects and then blocks. If the security can be affected a lot from any application or software ,firewall automatically deletes that application or software completely form whole system.

Use an inconspicuous network name (SSID)

Wi-Fi is one entry-point hackers can use to get into your network without setting foot inside your building because wireless is much more open to eavesdroppers than wired networks, which means you have to be more diligent about security. But there's a lot more to Wi-Fi security than just setting a simple password. Investing time in learning about and applying enhanced security measures can go a long way toward better protecting your network.

Use Enterprise WPA2 with 802.1X authentication

One of the most beneficial Wi-Fi security mechanisms you can put into place is deploying the enterprise mode of Wi-Fi security, because it authenticates every user individually: Everyone can have their own Wi-Fi username and password. So, if a laptop or mobile device is lost or stolen, or an employee leaves the company, all you must do is change or revoke that particular user's log-ins. (In personal mode, by contrast, all users share the same Wi-FI password, so when devices go missing or employees leave you must change the password on every single device — a huge hassle.)

Use rogue-AP detection or wireless intrusion prevention

We have already touched on three vulnerable access point scenarios: One where an attacker could set up a fake Wi-Fi network and RADIUS server, another where someone could reset an AP to factory defaults, and a third scenario where someone could plug in their own AP. Each of these unauthorized APs could go undetected by IT staff for a long period of time if proper protection is not put in place. Thus, it is a good idea to enable any type of rogue detection offered by your AP or wireless controller vendor. The exact detection method and functionality vary, but most will at least periodically scan the airwaves and send you an alert if a new AP is detected within range of the authorized APs.

VLAN configuration recommendation

We configure VLANs using layer two technology built into switches. In addition to segmentation, VLANs also benefit from switch security capabilities. Switch manufacturers base their VLAN implementations on IEEE Std 802.1Q. Basic switches (IEEE Std 802.1D) operate at layer two (L2) of the OSI model. The OSI model, or standard, is the guideline for technology manufacturers who strive to build interfaces with other network technologies. System attack surfaces are not perfect. Consequently, we should allow only expected traffic to reach them. VLANs provide this capability. By using VACLs, entry into each VLAN is tightly controlled, and use of L3 ACLs helps ensure only authorized packets route between VLANs. Routing between VLANs is necessary. However, if all VLANs end up routed to all other VLANs, something is wrong in your architecture, and the benefits of network segmentation diminish. Securing VLANs includes both switch security and proper VLAN configuration. The most common attacks against VLAN technology, VLAN hopping and double 802.1Q tagging, are preventable with proper attention to configuration best practices. In addition, consider not using VTP or other automated VLAN registration technology. The risk usually exceeds the benefit. Send voice and data traffic via separate VLANs. Protecting voice packets requires the same diligence as that applied to securing data VLANs. Further, VLAN QoS tagging ensures switches process voice traffic first to avoid performance issues. Finally, enhance network segments by making them security zones. A VLAN by itself is not a security zone. Rather, a VLAN with appropriate monitoring and filtering eventually becomes a security zone.

Address Resolution Protocol

When a computer needs to communicate with another network-attached device, it sends an address resolution protocol (ARP) broadcast. This assumes the IP address, for example, of both devices possesses the same network identifier. For example, if the target device and the source device both have the network address 192.168.10.0/24, the source device safely assumes the target device is on the same network or network segment. The broadcast packet travels to all devices on the same network segment asking for a response from the device with the target IP address. An 802.1D (D-switch) receives a broadcast packet and sends it out all ports except the one on which it is received. The first issue is packet delivery to all devices. This unnecessarily increases network traffic and degrades performance. The second issue is visibility. The desktop device in our example can find any connected device simply by sending one or more ARP broadcasts. A D-switch enables maximum visibility because it cannot determine whether a requesting device is authorized to see or contact the target device. Further, all devices exist on the same network segment.

Laptop security configuration

In general, laptop security is a term for the various products and techniques used to prevent the theft of laptop computers. Laptop security solutions can involve physical lock-and-key systems, locator devices, or other kinds of items that make it difficult for thieves to steal laptop computers. Here are five simple, but critical steps to protect your computer,

- Install Firewall (recommended).
- Install Antivirus Software.
- Install Anti-Spyware Software.
- Use Complex and Secure Passwords (recommended).
- Check on the Security Settings of the Browser.

IV. APPLICATION POLICY RECOMMENDATION

In this fast changing world, one needs better representation of work instead of hard work .

For representing the work one needs any of the two platforms either he/she uses website or may use a mobile

application. We had discussed website in above topics. So now let us concentrate on mobile application. There is much software's that are used to make a very good mobile application so that the people can share their information to one another. Today mobile applications are on a boom!!! As mobile application provide huge options to make desired application. But besides many people use them as to spread terror or to harm others. As they embed malicious scripts in them and as the application get downloaded the script also gets downloaded.

The scripts starts to perform desired work as the writer had written in it.

So to prevent our system we would require some counter-measures as follows:

I. Install antivirus available
II. Stay Updated with system and applications
III. Avoid activating the "install foreign application settings" setting in your system.

Most full IT security plans would include the following policy topics:(there can be more policies)

Acceptable Use Policy

Since inappropriate use of corporate systems exposes the company to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved. The scope of this policy includes all use of corporate IT resources, including but not limited to, computer systems, email, the corporate network, and the corporate Internet connection.

Confidential Data Policy

Confidential data is typically the data that holds the most value to a company. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data. This policy would detail how confidential data should be handled, and examples of what your organization deems confidential.

Email Policy

Email is an essential component of business communication; however, it does present challenges due to its potential to introduce security threats to the network. Email can also influence the company's liability by providing a written record of communications. Your email policy would detail your organization's usage guidelines for the email system. This policy will help the company reduce risk of an email-related security incident, foster good business communications both internally and externally, and provide for consistent and professional application of the company's email principles.

Password Policy

The easiest entry point to building your security policy, a password policy is the first step in enabling employees to safeguard your company from cyber-attack.

Passwords are the front line of protection for user accounts. A poorly chosen password may result in the compromise of your organization's entire corporate network. This policy would apply to any person who is provided an account connected to your corporate network or systems, including: employees, guests, contractors, partners, vendors, etc.

V. WIRELESS NETWORK AND GUEST ACCESS POLICY

Every organization should have a wireless policy that would likely need to include your guest access requirements. Wireless access can be done securely if certain steps are taken to mitigate known risks. Guest access to the company's network is often necessary for customers, consultants, or vendors who are visiting company offices. This may simply take the form of outbound Internet access, or the guest may require access to specific resources on the company's network. Therefore, guest access to the company's network must be tightly controlled. This policy would outline steps the company wishes to take to secure its wireless infrastructure. These policies would cover anyone who accesses the network via a wireless connection, guest included.

Intrusion detection and prevention for systems containing customer data

Intrusion detection and prevention are two terms describing application security practices used to mitigate attacks and block new threats. The first is a reactive measure that identifies and mitigates ongoing attacks using an intrusion detection system. It's able to weed out existing malware (e.g., Trojans, backdoors, rootkits) and detect social engineering (e.g., man in the middle, phishing) assaults that manipulate users into revealing sensitive information. The second is a proactive security measure that uses an intrusion prevention system to deterrent block application attacks. This includes remote file inclusions that facilitate malware injections, and SQL injections used to access an enterprise's databases.

VI. CONCLUSION

By applying all above discussed methods of security in one's day to day life. It can remain secure and able to data secure i.e., personal level privacy can be maintained. As we all know that the world is changing so fast, and the computer's age is growing faster than the world. So, there are almost every day or every week a new security arises. Governments and the Tech Enthusiastic are working at their level best to make everyone more secure and trying to increase the security so that everyone's private data can remain private and safer to use.

REFERENCES

[1] About the Internet Archive. Archived from the original on 2 October 2013. Retrieved 5 October 2013

[2] Pallab, Ghosh. 2015. "Google's Vint Cerf warns of 'digital Dark Age'". BBC News, Science & Environment.

[3] Donoghue, Andrew (19 July 2007). "Defending against the digital dark age". ZDNet. Archived from the original on 23 October 2012.

[4] Wearden, Graeme (27 February 2006). "Distributed computing cracks Enigma code". CNET News. Archived from the original on 19 December 2010.