PART A: SECURING THE COMPUTER NETWORK

Threat 1: Ransomware (RDP) attack:

K12 and some other companies that provide educational services report that there has been an increasing number of ransomware attacks on schools and universities in the last couple of years [1, 2, 3, 4, 5]. One of the main reasons behind this rising threat is the increasing demand for online learning (natural globalization trend, but the COVID-19 pandemic boosted this need) [6]. This remote access scheme created a giant problem for educational institutions in terms of cyber security [7]. Our school also falls into this risk category because "remote access" is one of the main requirements for our computer system. The use of remote access and the popularity of the Microsoft operating systems lead to the increased use of the remote desktop protocol (RDP). RDP is a proprietary Microsoft protocol (Linux has xrdp) that enables remote connection between the Host and Client machines through a secure encrypted tunnel [8]. The criminal can search and find a device with an open and insecure RDP port (network service channel, default TCP port 3389). Using this port, a criminal can establish a connection that may not raise suspicion, scan the network he accessed and create a bridgehead (command and control communication through another RDP connection) to deploy ransomware (or any other malware) to the server. Ransomware is designed to block access to files, usually by encryption, followed by the demand for payment. In our case, it means the choice between the loss of all information (student and staff personal information, grades, communications, etc.) or the loss of money for ransom pay[9, 10].

We can use several measures to protect our computer system from this type of attack:

1. Change the default RDP port number to another (we can do it manually or using special tools). Such a move will effectively "hide" our device from the criminals that scan for the target using the default port value 3389.
2. Update Windows using the latest security patches to ensure that most known vulnerabilities (for example BlueKeep [11]) and exploits are taken care of.
3. Use strong passwords for accounts that can connect through the RDP and change these passwords regularly. This measure lowers the chance that criminals will get access to the network.
4. Set a safe "layer" between the school server and the external users that connect from the outside using a virtual private network (VPN). These measures add another level of protection to the system and prevent direct connections between a client and a server.
5. Set up a multi-factor authentication system for all accounts that use RDP. So even if a criminal gets access to the computer, he will not get access without a second device (phone or authentication token).
6. Even if we can't use cloud servers we should think about creating our own isolated data storage that will hold the backup data. So even in the worst-case scenario, our school will be able to restore or partially restore lost data.

Threat 2: Phishing attack

Another threat that commonly targets schools and other educational establishments (nearly 60% experience it in some form) is phishing [12]. Phishing is a socially engineered attack that tries to lure the user into the trap by pretending to be a legit service (it is called "spoofing")[13]. To be precise, most malware attacks start from phishing probing (emails, websites, etc) [14]. Phishing can take different forms: a website that imitates a real service and asks for your login information, an e-mail from the "verified" source that asks you to download something or redirect you to another website, social media post or page, or even a phone/skype call to "confirm" something [15]. Phishing attacks often use “Gmail” service, because it is free to register and holds a solid reputation [16]. So potential phishing attack on our school can look like this:

- Criminals look up information in open sources to find information about our school - names, addresses, phones, emails, and other information about our staff, board of directors, students, etc.
- It uses this information to start a massive campaign with messages about real legit topics. For example, every student and/or teacher receives an email from the "healthdepartment.universityname@gmail.com" titled "Regulations updates concerning COVID-19". It can even contain a real name, titles, and some information about the school that the criminal acquired on stage 1.
- This message contains a link to complete a survey on your current situation.
- Among other, normal questions there are several that question your data: name, address, student number, etc. In the end, it asks you to submit this information and links to another page that imitates our school's website login page. After the user enters his credentials website thanks you for your participation and suggests that you read the information provided in the pamphlet. Simultaneously all your data and login information will be sent to the criminals.

The leak of sensitive information can create a breach in school security (login data with high access level can compromise our system), or cause a loss of prestige case of a data leak.

1. The initial step of phishing protection is to create a barrier between the target and the criminal. It can be done by hosting a personal email server for students and personnel, which will less likely show up in open sources (people are more likely to use their personal emails for social media, not the specific ones). And we can set up anti-spoofing and anti-phishing to protect our users from malicious contact.
2. Because this type of attack is "social" in nature the best defense against it - is improved awareness. All parties must be regularly informed about the risk of phishing attacks and taught how to recognize and report them. If people protect their information and avoid falling for the scam, there is nothing to worry about.
3. The last "line of defense" against phishing is multi-factor authentication, so even if the offender gets personal login information - he will not be able to get access to the personal data and cause real damage.

Threat 3: Trojans

As I explained early, different threats are often used in conjunction to maximize the chances and the effect of the attack. Phishing is often used as an entry point, that opens up the victim to the second payload in the form of ransomware or trojan (for example second link in our previous phishing email example that contains a file with trojan). Trojans take up a very big part of all attacks targeting schools. Malwarebytes Labs report that trojans took up one-quarter of the threat detections on school endpoints in H1 2019 [17]. Two of the most prevalent families of trojans that target educational institutions are TrickBot and Emotet that been used to steal more than 1 bill. dollars [18, 19]. Trojans trick the user into executing the malware file by pretending to be something else (for example a document file, or spreadsheet). These files contain malicious code in form of script or macros, which will start a stealthy download of trojans components (in the form of Dynamic Link Libraries or DLLs). The malicious activities may vary, but often trojan monitors the user traffic, and if it detects that a user visits a certain resource (for example banking service or online shopping) it steals user data. The user is oblivious to the fact that his device is infected and continues to use it as normal, while the trojan is actively spreading through different means - through connected devices and networks using a vast amount of vulnerabilities and exploits to spread as far as it can. This characteristic is what makes this type of attack very dangerous for our computer system. Our system was developed to give access to different devices and handle both local and online connections. One of the most notable threats to cybersecurity is unsafe devices [20]. Many different platforms mean more exploits and vulnerabilities the criminals can abuse, and even if we protect our network from remote attacks (Threat 1) the user device can be infected beforehand, and then when the device is connected to the local infrastructure it can spread from inside, like a real "trojan horse" and steal or damage our computer system.

To protect our school from this threat I suggest several actions, besides the ones mentioned early:

1. All devices must be set to regular automatic updates, and this option should not be toggleable by the user. This way we reduce the number of vulnerabilities that trojans can abuse.
2. Install antivirus software (Norton, Avast, McAfee, Kaspersky, etc.) on all loaned devices and recommend this software for personal devices. AV software offers a level of protection of the internal processes and can prevent the trojan from injecting itself into the device process and warn the user if a threat has been detected.
3. Set up the firewall for the school network and regularly monitor traffic, especially accounts with high access levels. Almost every malware can be identified by the unusual traffic it generates, and trojans are no exception.

Literature and references:

1. https://www.k12dive.com/news/with-k-12-cyberattacks-expected-to-worsen-in-2022-what-can-districts-do/617677/
2. https://edscoop.com/texas-school-paid-547k-ransomware-jam/
3. https://www.arnettechnologies.com/athens-school-district-paid-ransom/
4. https://theconversation.com/cybercriminals-use-pandemic-to-attack-schools-and-colleges-167619
5. https://www.alvaka.net/wp-content/uploads/2021/05/Case-Study-School-District-Paralyzed-by-Ransomware.pdf
6. https://www.forbes.com/sites/quora/2021/07/22/how-the-pandemic-has-accelerated-demand-for-online-education/?sh=600267514774
7. https://www.zdnet.com/article/remote-working-has-changed-the-rules-of-the-workplace-so-watch-out/
8. https://security.berkeley.edu/education-awareness/securing-remote-desktop-rdp-system-administrators
9. https://usa.kaspersky.com/blog/history-of-ransomware/24514/
10. https://www.ketk.com/news/education/athens-isd-pays-50k-for-release-of-data-in-ransomware-attack/?web_view=true
11. https://www.welivesecurity.com/2019/12/17/bluekeep-time-disconnect-rdp-internet/
12. https://elearningindustry.com/anti-phishing-awareness-tips-for-education-sector#:~:text=In%202020%2C%2060%25%20of%20educational,correspondence%20comes%20from%20a%20cybercriminal.
13. https://www.ncsc.gov.uk/guidance/phishing
14. https://www.netwrix.com/download/collaterals/2021%20Netwrix%20Cloud%20Data%20Security%20Report.pdf
15. https://www.thesslstore.com/blog/10-types-of-phishing-attacks-and-phishing-scams/
16. https://www.techrepublic.com/article/how-phishing-attacks-are-targeting-schools-and-colleges/
17. https://blog.malwarebytes.com/trojans/2019/08/trojans-ransomware-dominate-2018-2019-education-threat-landscape/
18. https://techmonitor.ai/technology/cybersecurity/inside-trickbot-how-to-run-cybercrime-empire
19. https://heimdalsecurity.com/blog/emotet-malware-history/
20. https://theconversation.com/cybercriminals-use-pandemic-to-attack-schools-and-colleges-167619