Review of cyber threats on Educational Institutions

Jorge Pinheiro

Lusofona University of Porto, Portugal
jmiguelpinhiero@hotmail.com

Abstract. The aim of this paper is to review about the cyber threats on educational institutions. The paper will focus on summarizing the threats and explaining the problems that cyberattacks can cause, the origin of the attacks and what motivations can the hackers have to do this sort of things. Nowadays, the percentage of attacks to educational institutions is going up and there are many threats to institutions and even more dangers behind them. This paper will also show some suggestions to this problem that keeps terrifying the educational institutions in the days that we live and how to try to prevent them.

Keywords: cyber threats, educational institutions, attacks, dangers, hackers, prevention.

1 Introduction

Many of the day-to-day IT risks originate within the company or institution in question. They may consist of leaks of information from their employees, students or even teachers, which intentionally or involuntarily disclose passwords, sensitive information or actions from people with bad intentions within the institution, such as a student who wants to take advantage of their access and knowledge to gain entry into college networks or an employee who wants to harm something because he was fired, and forgetfully, the institution did not delete that person's data.

Educational institutions are a real gold mine for cybercriminals [1]. These store thousands of information from each student, teacher and staff. Bank accounts, addresses, school transcripts and other valuable data. Formerly the institutions were not attacked, but today that has changed.

There is a doubt that brings concern to universities, schools and other educational environments and it's why the area of education is so hit by cyber criminals, and one of the explanations is in the public that frequents these institutions. The fact that some students and teachers use computer labs and there is a risk of misuse is one of the main factors. Even if unintentional, a simple student can undermine the systems and information of an institution for a slight failure or bad use of their mobile phone for example. This same student when connecting to web pages or giving permissions on untrustworthy websites may be opening doors for hackers to enter.

10.11228/dpsc.02.01.004

In an educational institution there are hundreds of students, dozens of teachers, dozens of employees and collaborators, and the greater the number of people, the riskier and harder to monitor the cyber security gets.
Another of the many risks that we will talk about is the USB (Universal Serial Bus) flash drives brought, for example, by a student or teacher that is very useful for both of them to store important files, but that is one of the main transports for the entry of viruses.
One of the most important security strategy points is to control network access and only let each type of user who enters the network see the information to which they are only entitled and allowed. This lowers the likelihood of malware intrusions or infections that can damage networks, systems, equipment, and devices.

Today, universities, colleges, and schools track digitally absences, attendance, and grades as well as confidential student and parent documents. This information is increasingly vulnerable and easy to attack since there is no truly effective data protection program.

In section 2 of this paper we will talk about cyber threats in educational institutions, with an example of a teenager who entered two softwares from two different companies, which kept confidential data from the school where he used to study and also will be presented different types of threats and their definition.

In section 3 will be covered about what can be done to prevent any cyber threat and includes some tips on how to protect the network of institutions and reduce the risk of attack.

In terms of origins and motivations, some important aspects of why hackers break into networks and steal information will be summarized.

2 Cyber Threats

Educational institutions today face unique security challenges unseen in other sectors, so cyber security must be a priority. In addition, these institutions have a large and complex network with a large number of switches, routers and single users, making keeping the system secure from cyberattacks is an extremely difficult task [2]. IT departments must address these risk areas and find ways to mitigate threats. A university, for example, may contain thousands of users. These users may enter the system through older, less protected hardware such as a computer or a mobile phone that may not have the features required to install the latest software versions to remain protected, thus leading to a high vulnerability to attack.

While the education sector continues to grow, more institutions continue to evolve and opt for digital solutions to check a student's performance, schedules or even monitor tasks and organize them, which is of great importance to hackers. While insti-

tutions continue to collect immense amounts of student information, the responsibility to keep this type of information secure also increases [3]. As a result, information carries a great risk of being attacked in a variety of ways, and hackers can find various ways to break into systems to gain access to anything that is valuable.

An example of cyber threats is the case of Bill Demirkapi who a few years ago, when he was in tenth grade, he was a typical hacker. A bored teenager who broke into the school network where he was going to change his grades [4]. At the DEFCON conference in Las Vegas [5] (one of the largest hacking conventions in the world), he presented his three-year breakthrough after-school hacking, which began when he was still a student at the school.
Demirkapi explored two types of software sold by two companies, Blackboard [6] (technology education company) and Follett [7] (company that deals with vital information), which were used at the school where he went. In both cases, he encountered serious bugs that could give a hacker deep access to a student's information. In the case of Blackboard, Demirkapi found 5 million vulnerable student and teacher data, including grades, balance to spend on school, schedules, password hashes, and photos. He himself stated that if he were not a young man motivated by his curiosity, he could so easily enter corporate databases, his story does not quite demonstrate the security that exists in these companies, which have millions of personal information from each student.
“The access I had was pretty much anything the school had. The state of cybersecurity in education software is really bad, and not enough people are paying attention to it”.

The bugs that Demirkapi found in both companies were very common on websites, including SQL injection and cross-site scripting vulnerabilities. Detailing each company, in the case of Blackboard, the bugs found gave full access to a database with 24 categories of information, with everything from phone numbers to bus routines done. The data belonged to over 5000 schools, with 5 million total data, including students, teachers and other staff. In the case of Follett, the bugs found in this software gave the hacker access to data such as grade point average, number of suspensions and passwords, which unlike Blackboard, were kept unencrypted. When Demirkapi gained access to this level of information, he knew the risks of fraud and abuse that prohibited gaining unauthorized access to a company's network.
With this he asked a friend for permission to verify that the data he had matched the data he had obtained. Demirkapi neither explored nor counted how much vulnerable data he had discovered as he did with the Blackboard company. However, the companies were grateful that he found these bugs, and reported them, to fix all problems they encountered. But let's imagine that Demirkapi, instead of doing what he did to help companies, kept the data. All the data found could have fallen into the hands of others who could use this sensitive data to make money.

In the next topic, we'll talk about some types of threats that exist that can cause serious damage to institutions.

2.1 The real danger for educational institutions

Technology developments and constantly changing transformations open many possibilities for educational institutions, but also increase the vulnerability and risk of hacker attacks [8]. Misuse or involuntary mistakes made by someone within the institution is one of the major problems seen by the values above. This leads us to think that institutions should take security measures and inform students, teachers and staff of the great risk of misuse of technological devices and devices. With each passing year, it can be said that the compromise of personal data and sensitive data in institutions increases compared to previous years.
Schools, colleges, and other educational establishments store a wealth of valuable student, parent, and staff information, including personal information, financial data, and even study materials.

Each year schools make the transition to the cloud and the security is left behind. The adoption of cloud technologies means security teams must be able to monitor suspicious and malicious activity from external threats.
The beginning of the school year means that thousands of students and staff will return to the institutions' cloud environments. It also means that thousands of pieces of information will enter and leave databases, which could lead to hackers having more reason to attack any of these institutions.

Educational institutions have a complex and distributed IT (Information Technology) architecture. Due to be a space open to all, there is a great diversity of public, which leads to having to provide zones of different virtual environments. This also means that everyone who is connected needs to be safe. For example, in a teachers' room, students, parents, staff and visitors to institutions cannot have access and can connect to that area. However, in other environments such as libraries, they are spaces that were made for exchanging information and ideas, so there will be a large flow of visitors and users coming in and out of the system. These environments pose a greater risk to the institution due to user behavior, whether intentional or unintentional. Misuse of computers, mobile phones, tablets and pens could pose serious risks such as damage to equipment, malware and the entry of users who should not have access.

But there is another problem, which are the holes in systems that make it easy to steal information or even change that sensitive information. Different types of data such as administrative, financial, and student records can easily be stolen or altered by anyone unknowingly. Therefore, in areas with high data transfer and little control over users, it is necessary to have devices or technological devices that can provide access, but not forget security.

There are different types of threats that are worrying and may cause disruption to educational institutions. Next, we will talk about some types and in the following topic, tips on what to do to protect institutions will be covered [9][10][11][12]:

- **Malware** [9][10]: This is the same as malicious software. It's any piece of software that was created to damage devices, steal information and usually create a great deal of confusion. There are different types of malware like worms, trojans, botnets and adware.

- **Worms**: Can infect a network of devices locally or over the internet using the network interface. Uses each machine affected to infect other people.

- **Spyware**: This is malware that was created to spy on a person. Hides in the background and takes notes of what this person does online, can include passwords, credit card numbers, what they usually search for, and more.

- **Trojans**: This type of malware masquerades as legal software or is hidden behind legal but corrupted software. It tends to act discreetly and creates backdoors on a person's security to let in other malware.

- **Botnets**: A network of infected computers that are under the control of a single main computer, all working together to accomplish a goal.

- **Adware**: While not always malicious in nature, this advertising software can greatly impair security, which can make it easier for other threats to enter.

- **DDoS**: Overloading a website or software with information that can give hackers a hint that can cause the site to become blocked and have to be shut down. It can be avoided with antivirus, firewalls and filters.

- **Phishing or Pharming**: Attempts to gain sensitive information that could lead to an intruder entering the network assuming identity of a legitimate source. Phishing is by email. Pharming is for fake websites and servers.

- **Ransomware**: It aims to hijack the computer by blocking its access to your machine's system and charging a ransom amount to free access.

- **Scareware**: Also known as cheating software, scareware may appear as legitimate notifications from antivirus companies, claiming that the computer has been infected and needs new software. However, by downloading the new program, personal information and passwords are stolen.

- **DNS Cache Poisoning**: It is the poisoning of the DNS protocol of the machine. This technique can be used to direct users from one site to another criminal, which may contain malicious content.

3 Cybersecurity care in educational institutions

Many institutions unfortunately feel that opting for information protection measures with new technologies and investing in the newest solutions on the market is better than lowering the costs of information technologies and not having consequences behind those costs [13]. What happens is, funding to fix an error caused by an attack or malware gets more expensive than a solution that allows prevention, maintenance and periodic updates. If we make a quick comparison between these two, it is better to have a system in place to protect the information and updates needed than to pay for a database that has been damaged due to an attack that could have been avoided if we were properly prepared.

Even if the institution has information security measures, it is not 100 percent secure due to a common factor, people. People are not perfect, so they can make mistakes at any time. But more importantly, they are behind security. To mitigate the risk of failures, vulnerabilities, risks of information loss, or misuse of sensitive information, security policies need to be implemented.

This information security policy should be adaptable to the organizational environment and the language used should be easy to understand for all hierarchical levels, from student to teacher. It is necessary to create a hierarchy for access to the information provided because there is data in the institutions that should not be seen by students or within the reach of teachers. There are also certificates that can be obtained by testing to show the quality standard or the safety standard, and this can be a very important aspect for the customer. For example, if one institution has no certificate and the other has some type of certificate or quality standard, it is obvious that the client will choose the most qualified and the one, that shows them, the most requirements for data protection.

Following are some tips on what you can do to try to reduce the risk of attacks and how to protect educational institutions [14]:

- **Educate teachers, students, and staff**: Defining and enforcing security policies is very important. This policy should include passwords, emails, internet, good use policies and other important variables. Depending on the technology and processes used, the goal is to define rules and procedures that all people in the institutions must follow while using the institution's Wi-Fi network and other devices. Once it has been defined and completed, the security policy should be published in various places, easily accessible areas of the institution and even shared on social networks as a way to reach everyone and with the goal of implementing the policy. as soon as possible. It is essential that staff and students always stay informed and perform monthly training to see if they can detect malicious emails and other threats.

- **Layer Security**: Schools, universities, and other educational institutions need to have an antivirus that can, learn, and update as new threats are found. It is im-

10.11228/dpsc.02.01.004

portant to create and implement security layers such as firewalls, filters, antimalware, system update applications, and create backups for strong defense against threats. This approach is a way to protect data and devices in ever-changing environments. If, for example, the antimalware system is compromised, there are additional layers to ensure the institution's information is secure and intact.

- **Keep software up to date**: Educational institutions use numerous servers and applications with vulnerabilities that allow hackers to gain easy access to the network. Keeping the system up to date can provide great protection for the institution.

- **Backing up data on the network**: If hackers gain control over sensitive information and threaten to encrypt or destroy it, a recovery and backup strategy is essential. Using automated backup and recovery software ensures data is kept safe and accessible from anywhere.

- **Monitor the network**: You can ensure visibility across the network. Being able to remotely locate vulnerabilities and correct them saves IT managers time and protects the network from costly and scale damage.

- **Beware of the websites you access and download**: Different types of malware can be found anywhere but, are more commonly found on sites that have little security. To reduce the risk of finding malware simply use sites with high security and reputation. Before downloading, always double check that the author is trustworthy and read the reviews and comments as the malware may be installing without us realizing it.

4 Origins and motivations

Educational institutions are one of the sectors most vulnerable to the risk of cyberattacks. In the first part of 2018, there was more than three billion compromised information overall, but only focusing on education, 9% of the cases belonged to this industry [15]. Because educational networks are home to the kind of information hackers want, and because the academic environment is often open, networks tend to be easier to penetrate and hackers have more than enough reason to attack institutions that are not ready [16]. Like other types of organizations, universities, schools, and other places of education contain extremely valuable data for hackers, such as citizen card information, credit card numbers, and even medical data from students, teachers, and staff. All information stored in an institution is not guaranteed to be secure if a cyberattack occurs. Many institutions let in any type of user (student, teacher, alumnus, partners, vendors) but this can lead to a risk that cannot be protected against connecting to the site by devices that do not have the necessary protection. Hacker's motives for attacking the network can be money, which is a major factor, but it can also be for espionage, to gain access to credential or sensitive data without anyone being

aware of it. One more reason for hacking is illegally search information that is extremely valuable and confidential. This information may have been provided by teachers for an important study or by a student and no outsider should be able to access this type of data, but this is a great motivation for the hacker.

One of the reasons why there is such a high vulnerability in educational institutions that the risk of cyberattacks is so significant is that there is a high exposure to external users. Information breaches can turn into serious issues such as identity theft, stalking and intellectual property violations. Several institutions have limited budgets for information technology infrastructures and teams. Universities and schools focus budgets on equipment needed for school and labs, for example, and not to protect the network from hackers because they store thousands of sensitive and extremely valuable data for them. Thousands of devices connect to the network of institutions and as technologies evolve, the protocols for their protection are becoming outdated. Attention must always be paid to updating the system and protocols, as well as always informing teachers, as they are easy targets for attacks. The large areas available and created for students and other members of an institution can be another target because anyone can easily access the network.

5 Conclusion

Human behavior is and will continue to be one of the reasons cybercrime happens, such as taking advantage of personal data to pretend to be someone with access to a major network, stealing bank accounts or even blackmail.
Unfortunately, despite existing precautions, it is highly likely that cyberattacks, due to their great diversity and evolution, will continue to be adversity in the future. Given that hackers fit into our society, they will be in constant progress, finding ways, even if institutions protect themselves properly, to corrupt the network even if they have obstacles.

During the development of this paper, the idea of prioritizing protection in educational institutions is extremely significant.
To enable the use of technology and innovation, educational institutions should take the necessary measures and implement strategies to protect themselves against potential cyberattacks. To reduce the likelihood of attacks on sensitive data stored in the institutions database, staff, students and teachers need to be properly trained against the type of threats and to be aware of all types of hazards that may be exposed.

Given all that has been developed during this research, I conclude that there are various types of threats as well as their solutions, but institutions still today do not give due value to cybersecurity which makes the risk of attacks is continually present.

10.11228/dpsc.02.01.004

References

1. Calegari, C. (2015). *Educação Lidera Ameaças a cibersegurança. Porque e como reagir?* Obtained from Grupo Binário: https://www.binarionet.com.br/blog/educacao-lidera-ameacas-a-ciberseguranca-por-que-e-como-reagir/ , last accessed: 2019/12/12
2. Regus. *Ameaças à Cibersegurança e a sua origem e risco.* (2016) Obtained from Work Portugal: https://www.regus.pt/work-portugal/cybersecurity-threats-where-do-they-come-from-and-whats-at-risk/ , last accessed: 2019/12/12
3. *Segurança da informação para instituições de Ensino: Qual a importância?* (2018) Obtained from AllEasy: https://www.alleasy.com.br/2018/01/10/seguranca-da-informacao-para-instituicoes-de-ensino/ , last accessed: 2019/12/12
4. Greenberg, A. (2019). *This Teen Hacker Found Bugs in School Software That Exposed Millions of Records*. Obtained from Wired: https://www.wired.com/story/teen-hacker-school-software-blackboard-follett/ , last accessed: 2019/12/11
5. Obtained from DEF CON (2019): https://www.defcon.org/ , last accessed: 2019/12/9
6. Obtained from Blackboard (2019): https://www.blackboard.com/ , last accessed: 2019/12/9
7. Obtained from Follett (2019): https://www.follett.com/ , last accessed: 2019/12/12
8. *The Education Sector And The Increasing Threat From Cybercrime*. (2019) Obtained from SentinelOne: https://www.sentinelone.com/blog/the-education-sector-and-the-increasing-threat-from-cybercrime/, last accessed: 2020/01/10
9. *Common Types of Cyberattacks in Education and What We Can Learn from Them*. (2017). Obtained from Fortinet: https://www.fortinet.com/blog/industry-trends/common-types-of-cyberattacks-in-education-and-what-we-can-learn-from-them.html , last accessed: 2019/12/11
10. Basic survey on Malware Analysis, Tools and Techniques Dolly Uppal, Vishakha Mehra and Vinod Verma: International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014, last accessed: 2019/12/11
11. A Dynamic Malware Analysis for Windows Platform - A Survey M. Asha Jerlin and C. Jayakumar: Indian Journal of Science and Technology, Vol 8(26), DOI: 10. 17485 /ijst/ 2015/ v8i26/81172, October 2015, last accessed: 2019/12/11
12. Grimes, R. A. (2019). *9 types of malware and how to recognize them*. Obtained from CSO: https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html , last accessed: 2019/12/11
13. *Cybersecurity tips for schools*. (2019). Obtained from Avast blog: https://blog.avast.com/pt-br/cybersecurity-tips-for-schools , last accessed: 2019/12/9
14. Fraser, J. (2018). *Ameaças Cibernéticas: Por que o Setor da Educação é tão Atrativo?* Obtained from Marsh: https://www.marsh.com/br/insights/risk-in-context/ameacas-ciberneticas--por-que-o-setor-da-educacao-e-tao-atrativo.html , last accessed: 2019/12/11
15. Breach Level Index H1 2018 Infographic. *The reality of data breaches.* (2018) Obtained from gemalto, a Thales company: https://safenet.gemalto.com/resources/data-protection/breach-level-index-2018-h1/ , last accessed:2020/01/11
16. *3 reasons higher education is a cyberattack favorite.* (2019) Obtained from onelogin: https://www.onelogin.com/resource-center/topics/3-reasons-higher-ed-cybercriminals , last accessed: 2019/12/12