2019

Cybersecurity-Beyond Data Protection

Amy J. Ramson
CUNY Hostos Community College

EZ TECH ASSIST

Cybersecurity: Beyond data protection

Published: October 1st, 2019

This OER material was produced as a result of the CUNY Public Interest
Technology initiative.

Created By:
eztechassist
Cyber Security & Managed IT Services

Written & Presented By:
Shalom Cohen
SCohen@eztechassist.com

Cybersecurity: Beyond data protection

Security threats date back to the inception of the Internet. What started out as a simple project to connect several universities together for the purposes of research, grew to the behemoth of a global network we know now as the World Wide Web.

In 1958, the United States government created the Advance Research Projects Agency (ARPA) to focus on technological research. Its purpose was to stay ahead of the Soviet Union's technological advancement. In 1969, ARPANET was created out of frustration that there were a limited number of powerful computers in the country available to research investigators. In 1976, the ARPANET was expanded by connecting to the packet radio network (PRNET) using radio transmitters and receivers instead of phone lines. In 1977, the satellite network (SATNET) was added to this network and the Internet was born.

The original version of the Internet was not designed to be widely available, so security was not at the top of the priority list. However, it was hard to use and information was difficult to find. Finally, in 1990, Hypertext was introduced, better known as hypertext markup language (HTML) a.k.a. the web page. By 1993, web browser software became widely used as the navigation tool of choice by users on the World Wide Web.

In the mid-1990s, companies like CompuServe, America Online and Prodigy began offering consumers with Internet access and e-mail.

Early Hackers were really programmers trying to improve computer tasks or fill software gaps. They created "hacks" in attempts to fix computer software problems and gain a better understanding of how computers work. In the mid-1980s, computers were being sold to the masses along with modems, which enabled the computer to connect to the Internet via phone lines. It was during this timeframe that some Hackers decided to use their skills for criminal activities.

Original crimes consisted of commercial software and games copied and distributed over the World Wide Web. Malicious Hackers, known as "black-hatters", developed viruses that shut down computers and networks. Until the 1990s, criminal hacking was not illegal. In 1986, the United States Congress passed the Federal Computer Fraud and Abuse Act, which made computer tampering a felony crime. Hackers that dedicated their efforts to solving problems were called "white-hatters". Today, hackers working at Microsoft Corporation to find vulnerabilities in Windows are known as "blue-hatters".

The Internet was designed as an open system, based on open source, encouraging universal access and giving anyone the ability to learning and understanding the technology. The Internet at its simplest form is the web page. When you open a web page, your computer downloads all the elements that make up that page, which include images, video, text and small programs. This opens the door for Hackers to plant malware on your computer.

Hackers gather at DEF CON and Black Hat every year. Both conferences, however, attract different types of Hackers. DEF CON is organized by Hackers for Hackers who compete on breaking into systems. Black Hat is more focused on education with presentations and classes on security techniques. There are many Hacker conventions held all over the world that attract security professionals from both the public and private sectors. There are also freelance Hackers that sell their services to individuals or corporations for the purposes of malicious intent and others for legal work. Legal hacking as otherwise known as ethical hacking, where companies hire a Hacker to test their computers and Internet defenses against malicious attacks.

Hacktivists (hacker-activists), like Anonymous, use denial-of-service (DoS) attacks to get their political massages across. DoS attacks focus on overloading a web site's server, causing the server to come to a complete stop. Another form of DoS is the distributed-denial-of-service (DDoS) attack with the use of many computers collectively working together to bring down a server or an entire network. Hacktivists, cybercriminals and cyberterrorists use DoS to shut down access to critical infrastructure, financial institutions, government branches and the media.

The Internet Society's Online Trust Alliance (OTA) published its report *2018 Cyber Incident & Breach Trends Report*. According to its calculations, the worldwide economic impact of cybercrime was at least $45 billion (€37.4 billion) in 2018. To reach this figure, the OTA studied several reports about the state of cybercrime. One of the most shocking pieces of data is the fact that, according to the OTA's calculations, 95% of security breaches could have been prevented.

Hackers have successfully infiltrated large corporations dating back to the year 2000. Some of these famous corporations are:

2000 – eBay and Yahoo suffered DoS attacks
2006 – The personal information of over 650,000 AOL users were posted publicly
2007 – 94 million credit cards of T.J. Maxx shoppers were exposed
2008 – 134 million credit cards of Heartland Payment Systems users were exposed
2009 – Intellectual property of Yahoo and Google were stolen
2011 – 77 million accounts of Sony PlayStation network were hacked
2014 – Account information belonging to J.P. Morgan Chase customers were exposed
2014 – 56 million customer accounts from Home Depot were accessed
2015 – 14 million records of Anthem health insurance were accessed
2017 – 148 million consumer records of Equifax were accessed

Cyberbullying a.k.a. electronic aggression, is used to intimidate, harass and cause harm to victims over the Internet. The Center for Disease Control and Prevention (CDC) report between 9 and 35 percent of young people say they have been victims of cyberbullying.

These 2019 statistics on cyberbullying shed some light on how large the problem is becoming across the nation — for students and adults alike:

- 73% of students under 18 years old report being bullied at least once in their life.
- The number of students who feel bullied is now nearly double what it was in 2016.
- 87% of minors have seen cyberbullying online in some form.
- One in six women have been stalked online, and one in 19 men report online stalking.
- Out of every 10 American adults, four report experiencing harassment online.
- 15% of people report being a cyberbully at least once in their life.
- 69% of people report harassing or abusing someone else online, though they did not identify it as cyberbullying.
- 64% of students report that being cyberbullied affects their ability to learn.

The online channels where cyberbullying occurs can change rapidly. A 2019 study from Enough.org shows popular social media channels and their percentage of users that have encountered bullying incidents:

- Instagram: 42%
- Facebook: 37%
- Snapchat: 31%
- WhatsApp: 12%
- YouTube: 10%
- Twitter: 9%

Finally, Cyberwar is a phrase best known by world nations, whereby government computers are hacked causing disruption, for stealing classified information and/or maliciously attacked by another nation-state. NATO, a military alliance of North American and European countries, offers three conditions of a cyberwar attack:

1. Sensitive information is leaked of stolen
2. Information to its owners is blocked
3. A person dies as a result of the attack

The impact of a cyber breach is one of financial, brand, reputation and national security. It is expected that there will be approximately eight to nine billion public records by year 2020. There are currently an estimated two million job vacancies in cyber security. The volume of attacks is growing significantly, so security companies are developing new innovative approaches to mitigating these cyber threats by utilizing artificial intelligence and machine learning capabilities.

As responsible individuals we need to take precautions in protecting our own computers, smart devices and the Internet of Things (IoT) appliances. Today, every individual, corporation and government computer is susceptible to a hacker’s attack. Cybercrime is on the rise and will continue to wreak havoc for years to come.