Proceedings of the 5th World Congress on Electrical Engineering and Computer Systems and Sciences (EECSS'19)
Lisbon, Portugal – August, 2019
Paper No. CIST 116
DOI: 10.11159/cist19.116

Bring Your Own Device (BYOD) Also Brings New Security Challenges

Harrison Carranza[1], Aparicio Carranza[2], Syed Zaidi[1]
[1]Bronx Community College of The City University of New York (CUNY)
Bronx, NY, USA
Harrison.Carranza@bcc.cuny.edu; syed.zaidi@bcc.cuny.edu
[2]New York City College of Technology of The City University of New York (CUNY)
Brooklyn, NY, USA
acarranza@citytech.cuny.edu

Abstract - What once was limited to our personal computers has now grown to touch other pieces of our lives making us more vulnerable to attacks. According to Forbes's Cesar Cerrudo, "Some experts predict that by 2020 there will be 200 billion connected things; Cars, planes, homes, cities, and even animals are being connected." As these technological luxuries grow, so do our demands for instantaneous information, sometimes leading us to take down our guards. It's clear, cybersecurity is an issue and besides costing some their identities it can break a corporation at its core, as seen with the recent Equifax breach, as of September 11, their stock was down 18.4%. In this paper we will touch upon the different types of cybersecurity threats and some ways corporations can learn to be vigilant as the world grows and expands its networks. We will go over how to educate employees on issues such as e-mail phishing scams. On the corporate side of things, this paper will explain how to implement BYOD environments and next generation endpoint protection.

Keywords – BYOD, Cybersecurity, MDM Solution, Next Generation, Traditional AV.

1. Introduction

Network outages, hacking, computer malware, and similar incidents influence our lives in ways that range from inconvenient to dangerous. As the number of clients, digital applications, and information systems increase, so do the open doors for exploitation. Cyber security which is alluded to as data innovation security, concentrates on protecting systems, networks and data from unintended or unauthorized access, change or destruction. Government offices, corporations, financial foundations, clinics, and other groups gather, process, and store a lot of secret data on servers and transmit that information over systems to different computers. This has tragically expanded the danger of cyber-crime, and reports of significant data breaches. Because of this developing volume and sophistication of cyber-attacks, continuous attention is required to ensure secure business and individual data, and in addition defend national security. This had prompted the improvement of digital advanced procedures to gather permissible proof after cybercrimes, and help with recognizing and prosecuting those responsible. Bring Your Own Device (BYOD) strategy is the initial phase in bringing order out of personal device. A portion of the primary reasons organizations of today are so tolerating of BYOD in the work environment as a rule identifies with worker fulfillment and expanded efficiency. Representatives who are allowed to utilize their own particular gadgets in the workplace are for the most part more fulfilled and somewhere in the range of 43% of representatives interface with their emails on their cell phones keeping in mind the end goal to excel and facilitate their workload. On the other hand if users need to utilize their own particular gadgets, they need to take some broad rules for doing as such inside an organization. Security is a progressing procedure that requires cautiousness, correction, and adaptability. The worldwide market for BYOD reached $181.39 billion on 2017. While data protection evolves, organizations should remain educated on the advantages, dangers, and protection suggestions related with BYOD in the work.

BYOD was briefly introduced in Section I, in Section II we describe Bring Your Own Device, Next Generation Solution is described in Section III, following in Section IV Employee Education is emphasized and in Section V our Conclusion is presented.

2. Bring Your Own Device

BYOD has become a huge trend, with nearly a third of employees using personal devices at workplaces [1]. It is estimated to be valued at $366.95 billion by 2022 [2]. Employees may bring their own mobile devices for use with company systems, software, networks or information. BYOD can be beneficial for companies by increasing productivity, reducing IT and

operating costs, expanding the virtual employee base and retaining employees. However, all benefits aside, BYOD poses an increased information security risk, as a BYOD policy may lead to data breaches and increased liabilities for an organization. In order to ensure security regarding BYOD, companies must first create a policy. The policy should consider which employees can bring their devices, which devices will be supported, and the access levels that employees will be granted when using personal devices. Computer Associates, is a company which already has a great policy in place and suggests the following questions be answered for a more in-depth and personalized guideline.
Who will pay for the devices and data coverage required?
What regulations must be adhered to when using employee devices?
What measures will be taken for securing devices prior to use?
Where will data from BYOD devices be stored?
Will there be an agreement for employees that wish to bring their own devices?
What happens if an employee violates BYOD policy?
What privacy will be granted to employees using their own devices?
What support will the organization provide for BYOD users?
What safeguards are in place if a device is compromised?
What methods will be used for securing devices before they are retired, sold, or disposed of?

Once a strategy is in place it must then be sustained. BYOD maintenance is contingent upon a company's ability to coach its employees on best practices, device management and support, and enforcement of the policies [1]. The following tips are suggested when allowing employees to bring their own devices. This is to ensure the safety of the company and employees [1]. Use password protected access controls: Though many choose to ignore this first step, setting a unique password/access PIN, for each device is critical. Control wireless network and service connectivity: Employees should connect to trusted networks only. To avoid unknowingly connecting to unsafe networks, devices should be set to prompt users before connecting to networks. Control application access and permissions: IT and security teams should assist users in optimizing their access control and app permission settings so that each application can access only what it needs to function. Keep OS, firmware, software, and applications up-to-date: Software updates often contain security patches to protect users from the latest threats or exploits. Back up device data: Periodically backing up data will reduce the fallout should a device be lost or stolen. Enroll in “Find my Device” and remote wipe services: In addition to being able to track a missing device, these services usually have the ability to wipe a device remotely, a critical option for ensuring BYOD security in the event of a lost or stolen device. Never store personal financial data on a device: Employees should avoid saving any financial or otherwise sensitive data on their devices. Beware of free apps: IT and security teams can assist employees by providing lists of applications that are approved for download. Run mobile antivirus software or scanning tools: IT and security teams should assist employees in selecting and installing antivirus software prior to using their devices at work. Use Mobile Device Management (MDM) software as recommended by IT: Mobile device management software enables IT teams to implement security settings and software configurations on all devices that connect to company networks.

3. Next Generation Solution

3.1. Traditional AV Solution

Traditional antivirus programs have protected PCs and corporate networks from viruses and malware for decades. However, with advanced malware and technology, like smart devices, this has been difficult to do with traditional AV. AV programs have used signature-based and heuristics detection. Once a virus signature was identified, antivirus companies would blacklist that signature in their program by updating their virus definition. A report from Verizon’s 2016 Data Breach Investigation shows, “99% of malware is only seen once before hackers modify the code” [3]. Instead of antivirus programs actively protecting a PC from an infection, antivirus companies are writing signatures in conjunction to block that same malware.

Fig. 1: Illustration of traditional AV scanning and how it decides what is benign or malicious.

Fig. 1, illustrates how traditional antivirus software scans a document/email/website by comparing signatures and heuristics against the antivirus own signature and heuristics and from there is decided what to do with that document [4]. There are four approaches traditional antivirus uses to detect malware [5]: Pattern Matching, Behavioral Analysis, Heuristic Analysis and Hash Matching.

3.2. Next Generation Solution

Next Generation (NG) solution is an "evolution" of traditional antivirus or firewall that uses rules, behavioral analysis, and machine learning to detect threats, block, and protect your corporate network from cyber-attacks. To this day, traditional antivirus companies are using signatures to combat malware that have already been created. Traditional AV are unaware of a virus if it does not have a signature, whereas, a Next Gen solution has no signature and uses different methods to identify a threat. Next Gen solution evaluates malware with signature and no signature models. Although, malware can be executed, Next Gen solution records the behavior and eliminates the threat. As cyber-attacks become more and more sophisticated, so does the approach of Next Gen solutions. NG solutions have been making strides in the last couple of years detecting and preventing high profile malware, such as ransom ware, from penetrating computers and infecting data. Ransom ware is a form of malicious software that blocks access to your files until the attackers are paid. Payment is usually in the form of bitcoins and untraceable.

3.3. Antivirus on Steroids

As viruses and malware become more sophisticated and traditional antiviruses try to keep up with signatures, corporations are looking new ways to protect their network along their user's data. The solution is to use a system that does not require signatures but methods like behavioral analysis. Many companies have been dealing with ransom wares and paying perpetrators to recover data. Traditional AV programs are a step behind the malicious code writers. Next-Generation Antivirus (NGAV) uses a "system-centric view", taking into consideration every process, detecting malware through algorithms and preventing attacks in the future. NGAV examines not only the computer but the network and identifies vulnerabilities with this new solution. Initial setup is crucial as rules need to be applied for NGAV solution to eradicate the problem. However, once an NGAV solution is up and running, there is little to no involvement from IT Administrators. Fig. 2, shows the approach a next-gen solution takes in detecting, analyzing, and preventing malware from infecting a device. [4]

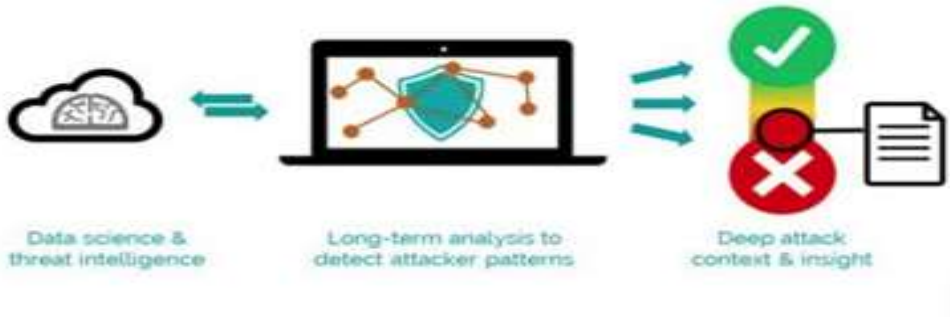

Fig. 2: Illustration of NVAG approach on detection, analyzes and decision/prevention.

NGAV takes four approaches to protect your business [4]: Prevents commodity malware better than traditional AV, Prevents unknown malware and sophisticated attacks by evaluating the context of an entire attack resulting in better prevention, Provides visibility and context to get to the root cause of a cyber-attack and provide further attack context and insight and Remediates attacks (traditional AV simply stops mass malware).

3.4. Differences between traditional AV and Next Gen solution

There are differences between traditional and next gen solutions. Due to advanced cyber-attacks, traditional AVs are unable to protect companies from these attacks. Although, Next generation solutions do use signature methods to evaluate threat, for the most part other methods also assist with identifying these threats. Normally, traditional AVs detect malware in the wild, it is analyzed at a central facility, so a signature can be created, the signature is packaged, and finally uploaded to the endpoint the following day. As for the next generation solution, the threat is either detected or not in the wild, it uses several methods to evaluate any threat, it identifies and destroys the threat from many methods, and the data is uploaded to a central repository for future prevention. Methods include behavioral, machine learning, and signatureless approaches that traditional AVs cannot do. Fig. 3, shows the difference between traditional and Next-Gen AV and the approach each solution takes [6].

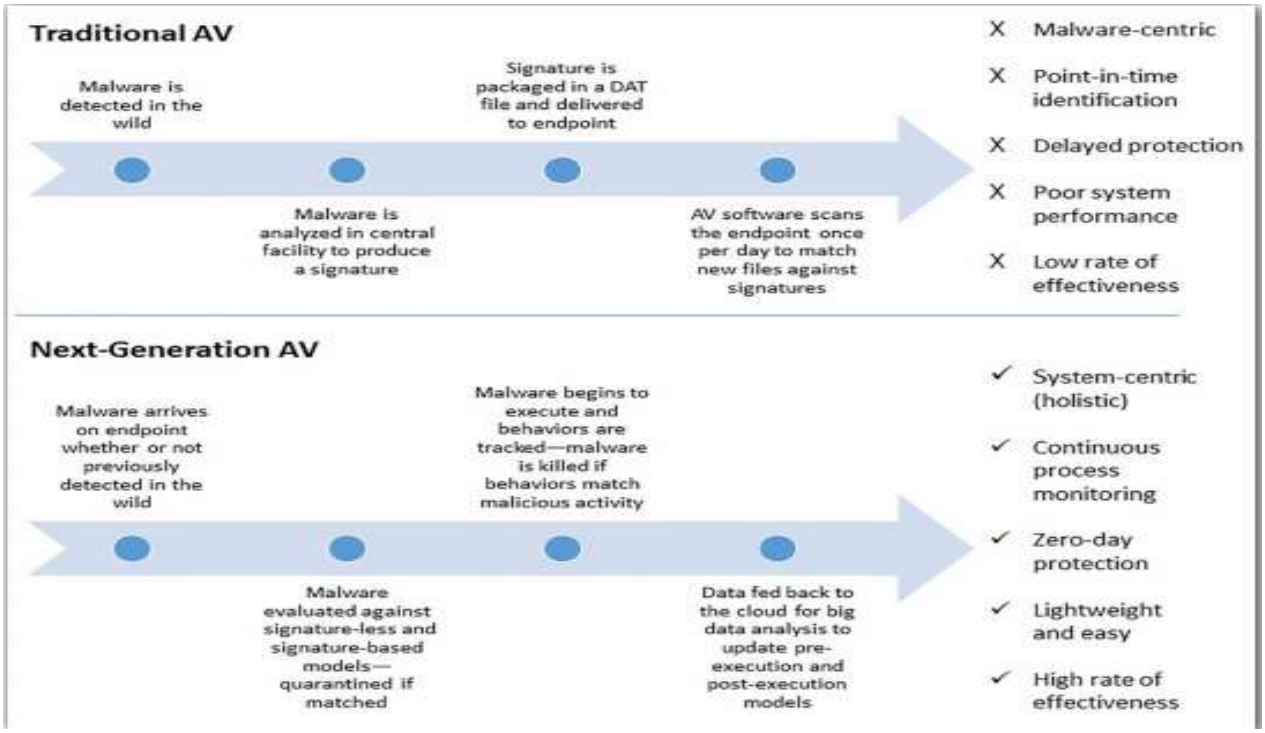

Fig. 3: Illustration of traditional AV process used to deal with malware compared to the Next-Generation AV solution.

3.5. Implementing MDM on BYOD

BYOD at the workplace is not a new concept, but it is becoming more prevalent in the corporate world. There are advantages and disadvantages for allowing BYOD in corporate networks. One advantage is for companies to save money by permitting users to use their own personal device. Another advantage, both for company and user, are presence and availability. With BYOD users are more productive because they are not limited to the normal business work hours of 8am to 5pm. As mobility brings information anywhere and everywhere, IT administrators need to implement new solutions to protect corporate data and network. For many of these companies, the question is how do we prevent data leaks and prevent privacy concerns. One answer to that problem is to implement a Mobile Device Management (MDM) platform. MDM is a platform that allows companies to control corporate services and resources on a user's personal device(s), such as a smart phone or tablet. The goal of MDM is to make sure that any device on the network is secured and protected along with corporate data. MDM is a platform that many vendors, such as Microsoft, have begun to offer to mid and large enterprises. MDM can be implemented on devices with Apple and/or Android operating system. Initial setup along with applying device certificates for security can be challenging and time consuming. Luckily, there are plenty of documentation to assist admins with this type of setup along with vendor support. Once, configured through Office 365, deploying it is not as arduous. Managing personal devices through MDM, like smartphones, are great for corporate security which helps mitigate any concern for data being compromised on local networks. If a user loses their smartphone or tablet, and it is linked to an MDM platform, the IT department can easily wipe "corporate information", such as Exchange. However, admins can also wipe an entire device, including personal and corporate information, to prevent any further corporate breach, as long as, the victim understands and accepts the consequences. Those consequences are losing important information that might not have been backed up.

4. Employee Education

Properly training employees is imperative on how to protect their personal data as well as understanding the risks when they or their children go online. This appears to be a significant gap in the focus of cybersecurity. Many companies are training employees on how to protect the company's data and perhaps securing their personal data, however they are not training employees on the risks particularly for children and teenagers using social media or texting online. We recommend either an online training course and/or printed brochures be provided to employees during orientation and periodically during their employment. The points below are important components [6]. Employees are responsible to protect the organization - They need to know that if a data breach happens due to their carelessness or lack of knowledge, they can be held accountable for not following procedures for protecting their laptops or other devices or for posting things online that compromise the company's reputation. If an employee has malicious intent, the person can not only be fired but also be subject to legal consequences. Employees should not lend their company devices to anyone including friends and family. Educate employees on the most common forms of attacks:

- ***(i)*** ***Social Engineering*** – Techniques used to get employees to share their passwords or other sensitive information,
- ***(ii)*** ***Phishing*** – Using emails with links to fictitious sites that collect a user's login information,
- ***(iii)*** ***Ransomware*** – The user loses access to their data until they agree to pay a fee to gain access back.
- ***(iv)*** ***What to do if you get hacked?*****[6] -** Get help immediately – call the help desk, change passwords on all accounts, Cleanse system using antivirus and malware tools**.**
- ***(v)*** ***How employees can protect themselves online?*****[6] -** Use different user IDs and passwords for financial information, personal tax information, email and social media sites, Edit the personal information you provide in online profiles. Remove high schools, maiden names and other information that only you know as these are used to reset passwords. Don't store highly sensitive data on your mobile device in case this device is lost or stolen. Use a webcam cover to prevent unauthorized access to the camera if your computer or device gets hacked. Ensure the antivirus or malware software is up to date and runs frequently. Install all software updates and security patches as soon as possible to reduce risk of known hacks.
- ***(vi)*** ***How employees can protect their kids from getting into trouble online?*** **[6] -** In addition to protecting the corporation and personal privacy, it is vital for employees to understand the risks that their children may be taking when engaging in social networking, text messaging and other activities that they may falsely believe is anonymous. It is important to include this because the majority of people are unaware of the types of risks that

may be occurring without their knowledge or understanding. Many parents are not aware of technologies such as Snap Chat, Instagram or even how text messaging can turn into cyber-bullying or be misconstrued and ruin a person's reputation.

5. Conclusions

BYOD is a critical new pattern that carries a variety of security questions, administration issues, and policy changes. By having in-depth learning of any concerns and dangers related with BYOD, assurance can nail down focuses and give fundamental safety required by business clients. Each of these risks represent a threat to organization's important and delicate information when appropriate safety measures are not set up. Before executing a BYOD approach at business, build up a security plan for employees to follow. Instructing employees on the significance of following directions can maintain a strategic distance from the danger of information being traded off. Because a bit of innovation like MDM is set up does not mean it can dispense all risk. Corporations should lead in-depth risk evaluations utilizing philosophies, these will help figure out what kind of security controls are suitable to ensure information and in some cases will indicate which data is too sensitive to put on a BYOD device at all.

References

[1] BYOD Security & Policies. (2018, December). BYOD: Bring Your Own Device, Secure BYOD Policies and Mobile Management. [Online]. Available*:* https://www.veracode.com/security/byod-security

[2] Globe News Wire. (2016, March). Bring Your Own Device (BYOD) Market size worth USD 366.95 Billion by 2022: Global Market Insights Inc. [Online]. Available: https://globenewswire.com/news-release/2016/03/22/822021/0/en/Bring-Your-Own-Device-BYOD-Market-size-worth-USD-366-95-Billion-by-2022-Global-Market-Insights-Inc.html

[3] J. Crowe. (2016, June). The clear-Cut Guide to Understanding Endpoint Security Software. [Online]. Available: https://blog.barkly.com/understanding-endpoint-security-software-landscape

[4] B. Johnson. (2016, 10 November). What is Next-Generation Antivirus (NGAV) | Carbon Black. [Online]. Available: https://www.carbonblack.com/2016/11/10/next-generation-antivirus-ngav/

[5] The Cylance Team. (2017, 15 May). How Traditional Antivirus Works. [Online]. Available: https://www.cylance.com/en_us/blog/how-traditional-antivirus-works.html

[6] B. Filkins. (2018, November). A SANS Guide to Evaluating Next-Generation Antivirus. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/old-new-replacing-traditional-antivirus-37377