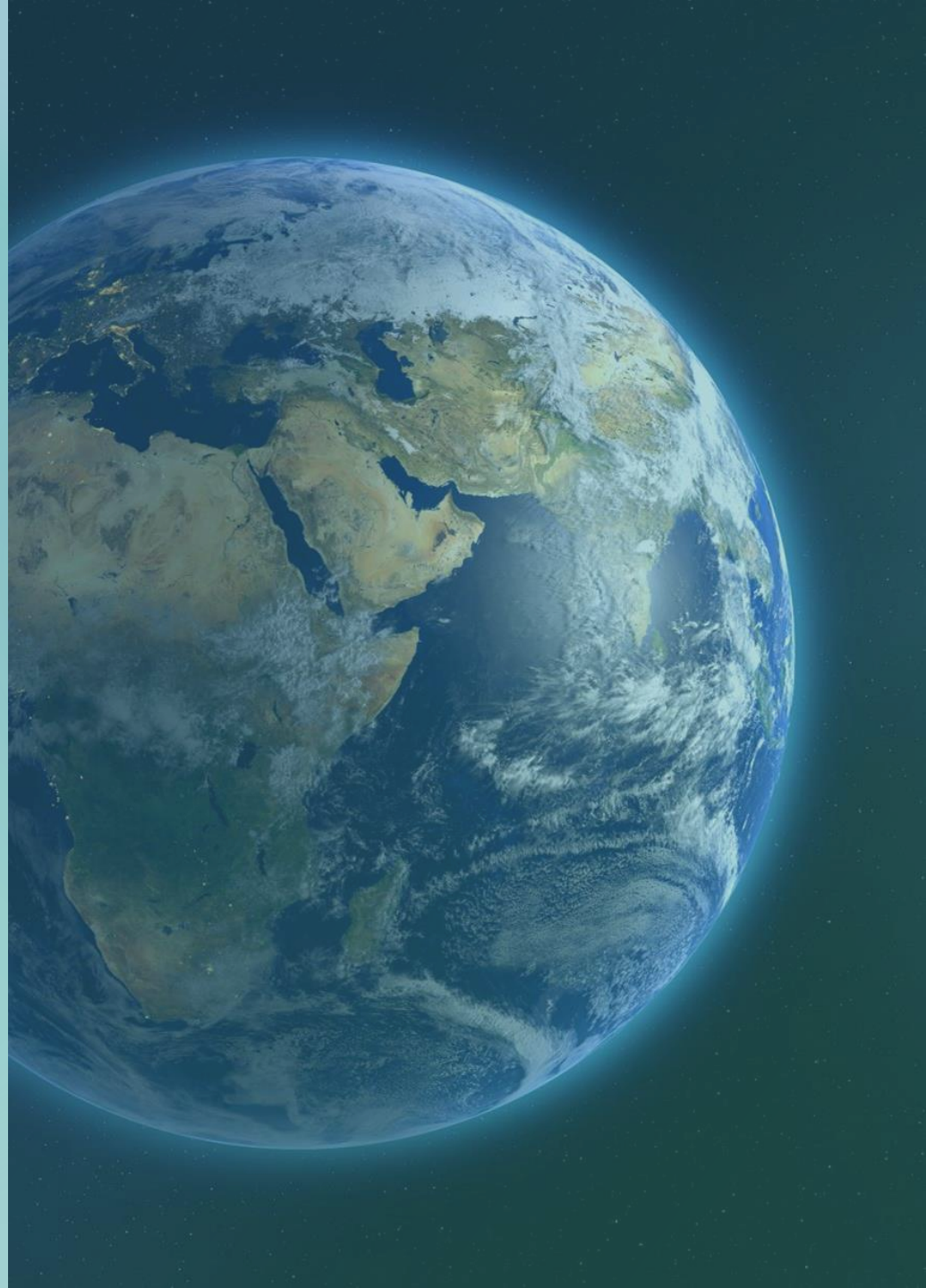
The Estée Lauder Breach of 2020

The forgotten records



Understanding Cybersecurity Breaches

When we think of security breaches most people may imagine Ethan Hunt breaking into a highly secure mainframe to still top secret information protected by the most sophisticated technology to prevent any possibility of theft. But this is far from the truth when it come to the reality of cybersecurity breaches. Many of these breaches are often due to human error in such things as poor password creation and maintenance, or a failure to protect the information all together.

Understanding Cybersecurity Breaches

Many of the hackers of today may not be who we think they are. Believed to be the youngest professional hacker in the world, Kristoffer Von Hassel, an 11 year old who said that he hacked into his Xbox One because he was desperate to get into games that he were not allowed to play. After the the discovery, Von Hassel's father, a computer system engineer, explained to his son the importance of bug ethics and presented his son with the option to do what was right by reporting his finding to Microsoft, or to post his findings on YouTube for everyone to know. He chose to report it to Microsoft. Von Hassel displayed characteristics of what we know of as an ethical hacker.

In the case of Estée Lauder

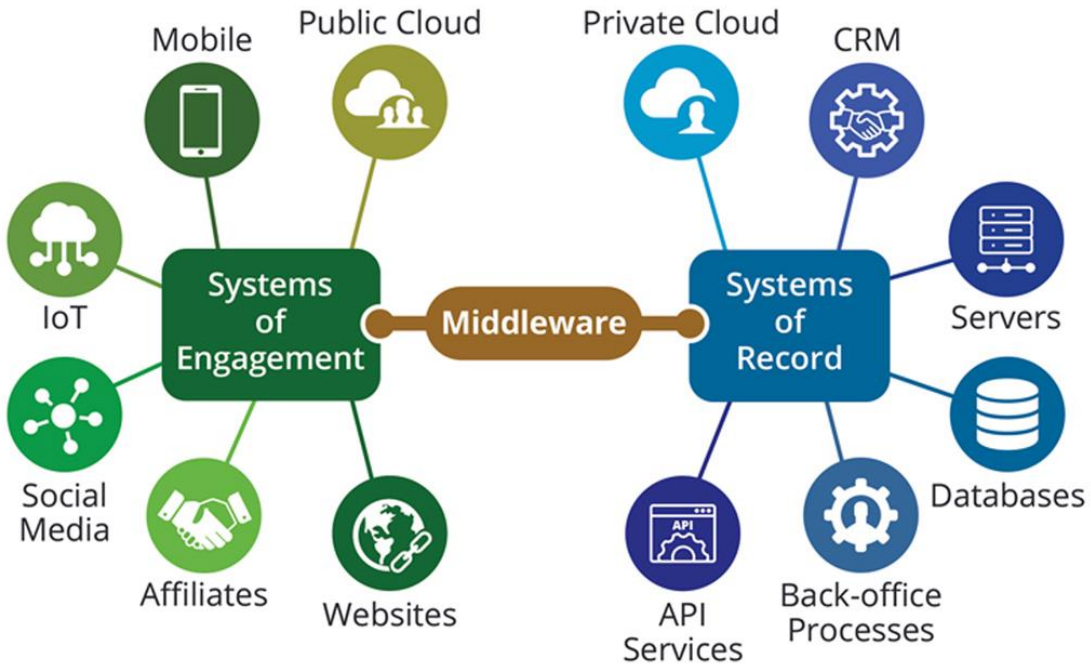
In regards to the breach of Estée Lauder, it was discovery found by security researcher Jeremiah Fowler on January 30th 2020. The findings revealed an exposure of a database of more than 440 million records. Though the company disclosed that the records were from an “education platform”, and did not contain any consumer data, the information did contain email addresses in plain text, reports, internal documents, IP addresses, ports, pathways, and storage information, which was accessible by anyone with an internet connection.

In the case of Estée Lauder

As we research the Estée Lauder breach further, we found that the internet facing database connected the New York-based cosmetic giant, was actually was not password protected. According to Fowler's findings this is a very common occurrence seen within large companies. In the case of Estée Lauder, it was found that middleware, such as, data management, application services, API management, and messaging, was discovered to be the cause of the breach.

Where the issue lies

In many cases when we discuss technology, we focus our attention on the network and the protocols we use to transmit data across it, as well as, the devices found at the network's edge, such as PCs, mobile devices, servers, and databases. Over the years we have seemingly gotten better at protecting our devices, but have failed at securing the services that help them communicate. Due to an increasing issue with properly protecting the data stored in devices on the outer edge of the network, such as databases and web servers; the discussion around middleware security is increasing growing.



Understanding Middleware and properly protecting the applications it touches

When working with web services we often here words tossed around such as REST (Representational State Transfer), JavaScript Object Notation, known as JSON, and SIMPLE Object Access Protocol, or SOAP. These frameworks are used by many middleware services to provide communication between different applications. In an expanding world of data collection and an advancing acceptance of connecting to the internet, middleware protection is more important than ever.

Protecting our data and the services used to manage it

Because businesses are continually trying to improve the services they provide to their customers, we have found that middleware applications such as **Red Hat JBoss Enterprise Application Platform, IBM WebSphere,** and **Oracle WebLogic,** are all used for helping with providing improved agility through, better user experiences, increased efficiency through automation, rapid innovation through shortening product development, portability and reusability by making applications scalable, cost effectiveness, and the most important, the management of information. Therefore this need for such services increases the risk in providing them.

- Popular Middleware Providers

Protecting our data and the services used to manage it (continued)

Because of the increasing need to provide better services to customers, the ability to protect their data has become more and more difficult. In the case of Estée Lauder, the issue was a simple human error of password protecting the middleware application used to manage one of their databases. But in the discovery of the breach, there was another issue that we need to mention. The fact that the database was internet facing. The easiest resolution would be to remove the database from the web, but this could prove to be time consuming and costly.

Understanding the vulnerabilities and the steps to remove them

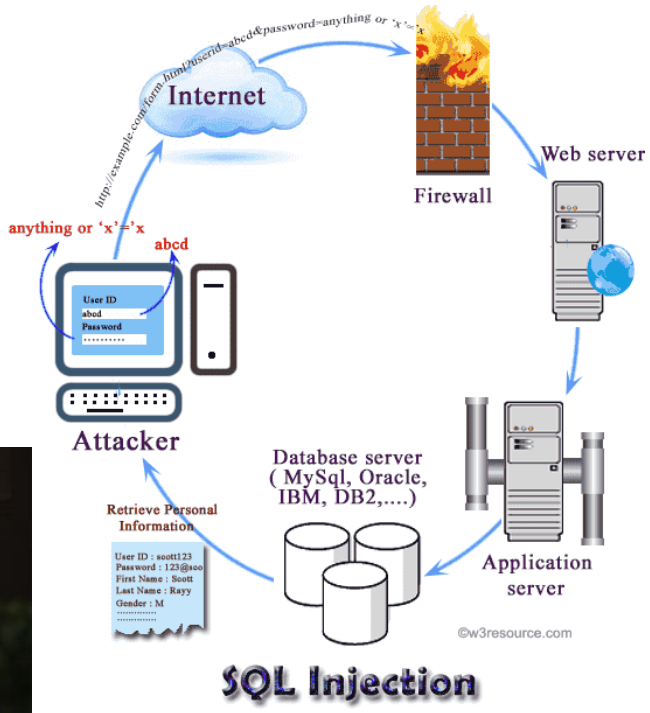
Now that we know that the obvious solution to preventing the breach of middleware access to web-facing devices, is not the best course of action. We must think of the best possible ways to secure the middleware, which is the gatekeeper of very important data stored in cloud and web servers, and databases. As we may consider all of the external attacks in our attempts to protect the companies data, we must also consider the possibly of internal attacks, by such ways as espionage, malicious intent from disgruntle employees, and sheer human error.

Understanding the vulnerabilities and the steps to remove them (continued)

What are some vulnerabilities that we should consider? Apart from simply creating a strong password to secure all devices and the middleware applications, other vulnerabilities we must consider are the possibilities of unauthorized user access to confidential data, no user authentication before accessing the applications, no data encryption on extremely sensitive information being transmitted, and improper coding during development. These are only a few of the many possibilities that can lead to vulnerabilities.

Securing the data we use and ways to do it

Today to the of the most common attacks are XXS Cross Site Scripting, which exploits JavaScript, and SQL Injections. These attacks normally exploiting laxed security practices during application development and middleware and all application setups. To prevent these types of attacks we should first consider securing the code that is used to build applications that will provide web services. Some preventions we can try are, creating strong passwords that does not use plain text storage. Use two-factor authentication which requires an authorized user to provide an additional form of verification other than a password, and giving minimum privileges to access sensitive data, amongst just a few.

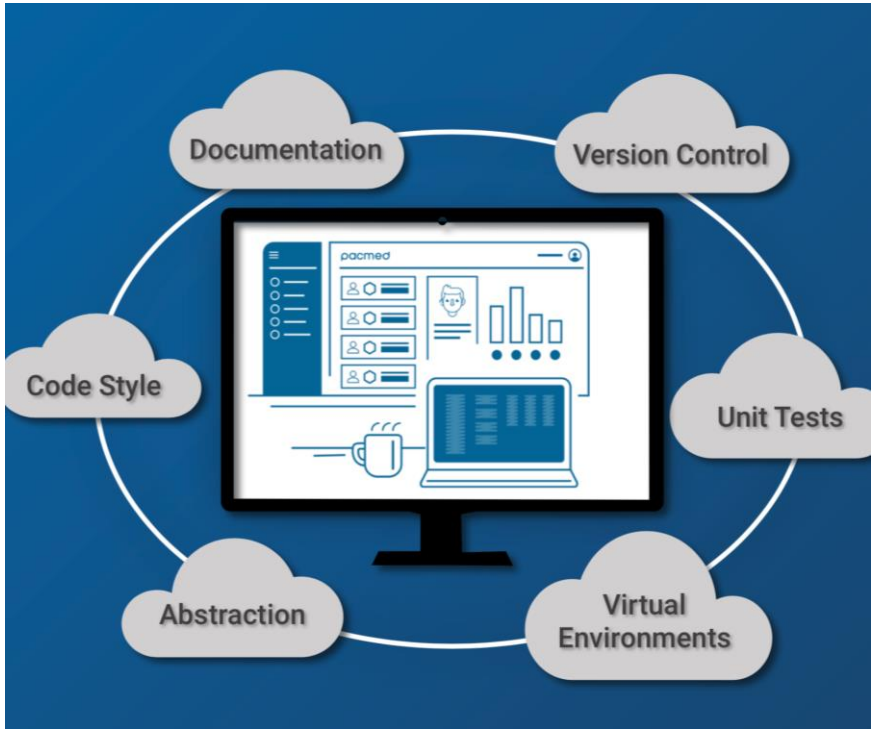


Securing the data we use and ways to do it (continued)

- In conjunction with user interactive security, the scripting side of securing the applications providing services also require very similar attributes during development. We can find in BASH, Perl, PYTHON, and JavaScript, scripting languages, that using specific best practices can help to secure applications from being exploit even if the middleware services has vulnerabilities..

Scripting best practices we all need to know

In BASH, ways that were can secure the application is first by considering the use of a higher level language, using set to set helpful options, and using quotes to prevent unexpected expansion. In Perl the use of the system(), exec(), open(), eval(), as well as, the PATH setuid, and race conditions, are all used secure the program from vulnerabilities. In Python, using the most recent version, using a virtual environment, and setting debug = to false, and never committing anything with a password, all helps to secure the program. And lastly, in JavaScript, protecting sites from XSRF (Cross Site Request Forgery, and XSS (Cross Site Scripting), requires the use of CSRF tokens on all state changing request and validate them on the backend, the use of same site cookie attribute, use custom headers, and verification of the origin with standard headers, and the placing of data in different slots to encode the sensitive data added in the site. The accomplish by adding several significant rules. Cross Site Scripting is the most intricate to implement of the two.



The success of security and prevention

As we consider the Estée Lauder Breach, we can see that there are several things that could have been done to ensure that no sensitive data was exposed. Of course in hindsight it is easy to make suggestions on how to fix these types of issues, but it has been proven that prevention is key to successfully protecting devices, applications, and services that connects them. In a day when concerns for data security is at its highest, we must ensure we consider proper scripting security, user input and authentication, data encryption, site security, on top of securing the devices connected to the network. Incorporating all these will hopefully in better protection, and the saving of time, resources, and money caused by unwanted data breaches.

Work Cited

- **References**

- “Cross Site Scripting Prevention - OWASP Cheat Sheet Series.” *Introduction - OWASP Cheat Sheet Series*, https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html. Accessed 5 Apr. 2021.

- “Cross-Site Request Forgery Prevention - OWASP Cheat Sheet Series.” *Introduction - OWASP Cheat Sheet Series*, https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html. Accessed 5 Apr. 2021.

- Henriquez, Maria. “The Top 10 Data Breaches of 2020 | 2020-12-03 | Security Magazine.” *Security Magazine | The Business Magazine for Security Executives*, Security Magazine, 3 Dec. 2020, https://www.securitymagazine.com/articles/94076-the-top-10-data-breaches-of-2020.

- “How Teenage Hackers Became Tech’s Go-to Bounty Hunters.” *The Hustle*, https://www.facebook.com/hustlecon, 26 Apr. 2019, https://thehustle.co/teenage-hackers-bug-bounty/#:~:text=Kristoffer%20Von%20Hassel%2C%20an%2011,’t%20allowed%20to%20play.%E2%80%9D.

- Lane, Adrian. “Strategies For Protecting Web-Facing Databases.” *Dark Reading*, Dark Reading, 8AD, https://www.darkreading.com/risk/strategies-for-protecting-web-facing-databases/d/d-id/1138203.

- Luenendonk, Martin. “What Is Middleware and How Does It Work? | Cleverism.” *Cleverism*, 8 July 2019, https://www.cleverism.com/what-is-middleware-and-how-does-it-work/#:~:text=Middleware%20includes%20software%20like%20content,to%20work%20on%20older%20systems.

- Winder, Davey. “Estee Lauder Database Exposed; Customer Data Not Involved.” *Forbes*, Forbes, 11 Feb. 2020, https://www.forbes.com/sites/daveywinder/2020/02/11/estee-lauder-data-leak-440-million-records-exposed/?sh=3b4901832590.