
Estée Lauder
Breach 2020
The forgotten Records

Understanding Cybersecurity Breaches & the Estée Lauder Breach

Who & what was the potential target?

The type of Institution

What systems were targeted?

What was taken and how?

Who was responsible and who was affected?

What was impacted?

Impacts to production

The lost of time and since of security

Economical Impacts

How the breach was addressed & protecting systems from future threats

Securing the data

Understanding the vulnerabilities

Tools for securing data

Understanding Cybersecurity Breaches & Threats

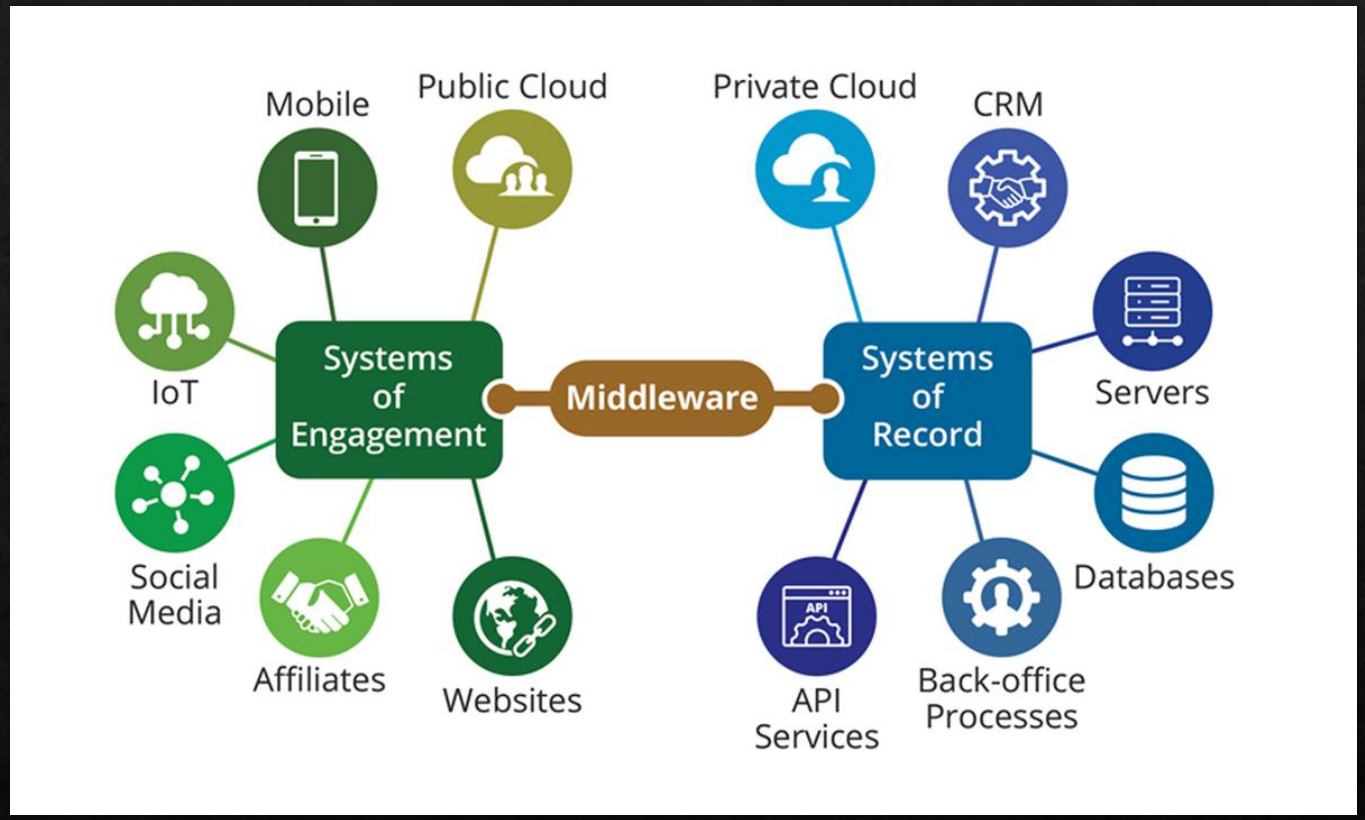
- There’s no specific profile for a hacker
- There is no system that can’t be hack
- With enough time and resources any system can be breached
- Access can be gained through:
  - Social engineering
  - Shoulder surfing
  - Scare tactics
  - Poor password creation
  - Poorly secured networks and device, etc.;

Who & what was the potential target?

- International Fashion & Cosmetics Corporation
- Customers
- Employees
- Potentially clients & vendors
- Internal systems & networks

Who & what was the potential target? Cont'd

- Middleware
- Data Management
- Application Services
- API management
- Messaging



What was impacted?

- Was there an impact on production?
- Was there an economical impact?
- Was there an impact to a since of security?

How the breach was addressed & protecting systems from future threats

- Securing the data
- Understanding the vulnerabilities
- Tools for securing data

How the breach was addressed & protecting systems from future threats Cont’d

- Ways to secure systems and protect devices from future breaches
  - Secure password
  - Multifactor authentication
  - Biometrics (finger prints, voice, retinal, facial)
  - Website security
    - VPN (Virtual Personal Network
    - DMZ (Demilitarized Zone)

How the breach was addressed & how to protect our systems from future threats Cont’d

Additional security tools and practices:

- Monitoring systems –
  - Solar Winds
  - Intruder
  - Syxsense
  - Acunetix
  - Wireshark

Cyber & data security best practices

- Require password changes every 60 days
- Require strong password
- Require the use of multi-factor authentication
- Require the use of a VPN to access network
- Use encryption when creating code
- Layered security

In Conclusion, “What did the Estée Lauder breach teach us?”

- Threats can come from anywhere, even from human error
- The benefits of testing regularly for security vulnerability
- Make sure to properly secure all data, with added security for highly sensitive data
- Insuring the proper setup and security of middleware applications
- Using best practices for continual prevention of breaches and attacks

Work Cited

References

Lane, A. (n.d.). Strategies For Protecting Web-Facing Databases, Dark Reading, 8AD. Retrieved from Darkreading.com: https://www.darkreading.com/risk/strtegies-for-protecting-web-facing-databases/d/d-id/1138203

Series, C. S.-O. (20, April 5). Introduction - OWASP Cheat Sheet Series. Retrieved 2021, from https://cheatsheets.owasp.org: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Winder, D. (2020, February 11). "Estée Lauder Database Exposed, Customer Data Not Involved" Forbes". Retrieved from Forbes.com: https://forbes.com/sites/daveywinder/2020/02/11/estee-lauder-data-leak-440-million-records-exposed/?sh=3b4901832590