Are Data Breaches Inevitable?

How do we mitigate the risks?

By Stephanie Duncan

11.12.2020

Contents

Mitigating the Risks of a Data Breach

It is imperative that organisations who utilise a network which has access to the Internet include the possibility of a data breach in their risk assessment.

A risk assessment should outline measures which should be taken in order to mitigate the risks of data breaches, as well as the inclusion of steps to be taken in the aftermath in the event that a data breach has occurred.

Not only do data breaches impact organisations financially, data breaches can also damage their reputation for many years which leads to long term loss of business.

Traditional Perimeter Based-Security

Traditional network security prevention methods include:

- Firewalls
- Anti-Virus Software
- Intrusion Detection Systems

As the number of organisations falling victim to data breaches increase, it is becoming clear that the above traditional methods are no longer adequate at preventing unauthorized users accessing their network.

Organisations must consider alternative measures to mitigate the risks posed by cybersecurity threats.

Cybersecurity Implications of Remote Working

Many organisations have been subject to an increase in exposure to cybersecurity threats and in turn data breaches, as a side effect of switching their employees from on-site to remote working. As a result, there has been an increase in demand for network resources and cloud applications.

According to a new study carried out by cybersecurity firm Malwarebytes, out of 200 IT-decision makers who were questioned, 20% of respondents said that a data breach had occurred within their organisation as a result of actions taken by a remote worker.

Furthermore, 44% of respondents' organisations failed to provide employees with cybersecurity training which outlined potential threats from working from home.

Phishing Email Cyberattacks

In March 2020, during the beginning of the COVID-19 pandemic, cyber threat researchers Barracuda Networks reported a 667% increase in malicious phishing emails which made reference to the coronavirus.

Effectively, many hackers took advantage of the focus on the pandemic in order to lure uncertain individuals into clicking or responding to these emails.

Twitter Spear-Phishing Attack

In July 2020, Twitter fell victim to a large hack in which a small number of employees were targeted with a phone “spear-phishing” attack. The hacker created a spear-phishing email which mimicked Twitter’s VPN, which prompted employees to log in to their accounts without suspicion.

The hackers were then able to obtain the employees’ credentials in order to access Twitter’s internal systems, which were then used to target 130 accounts.

Of those, the hackers initiated a password reset for 45 accounts and proceeded to login to the accounts and send tweets.

The hackers were also able to view email addresses and phone numbers of some users of Twitter’s internal systems.

FireEye Threat Actor Attack

FireEye, a Californian based security company which tracks the most advanced threat actors across the globe, recently announced they had been breached.

- Tools used to test their customers' security were stolen.
- According to FireEye, the attackers "used a novel combination of techniques not witnessed by us or our partners in the past."

This demonstrates the scale and evolving threat of cybersecurity attacks with the creation of sophisticated techniques by adversaries.

Cyber Essentials Scheme - Basic

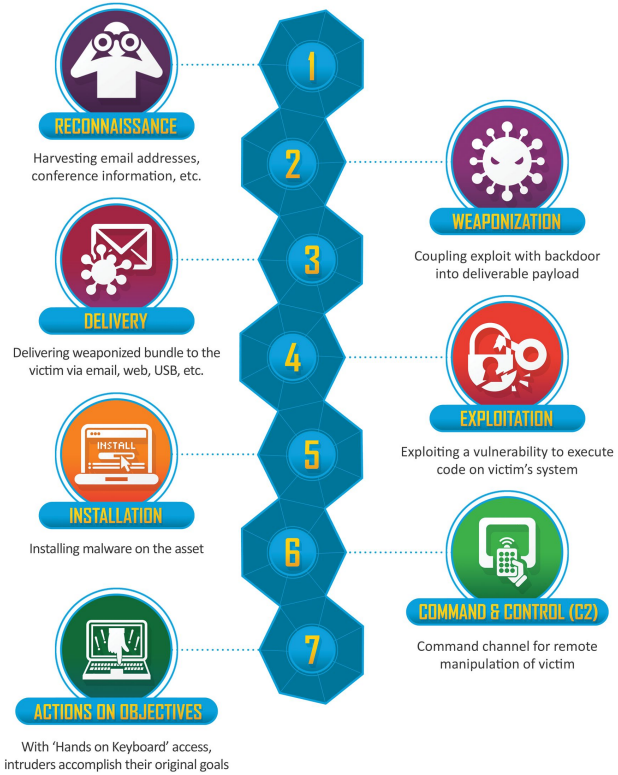
Launched in 2014, Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against common cybersecurity threats.

- Available for all organisations, regardless of size or sector
- Includes a basic set of technical controls
- Organisations can gain one of two Cyber Essentials badges
- Cyber Essentials Certification is a requirement for some government contracts
- At the very most CE would prevent a very basic threat, however the CE scheme is a good foundation.

Lockheed Martin Cyber Kill Chain

- Designed by Lockheed Martin, the Cyber Kill Chain model identifies what adversaries must complete in order to achieve their objective.
- Essentially, the chain of attack can be broken by stopping adversaries at any stage
- An intruder can only be successful if all six stages in the model are successfully completed.

Lockheed Martin Cyber Kill Chain



Lockheed Martin. Digital Image Retrieved From https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

MITRE ATT&CK - Advanced

- The MITRE framework can be used by organisations to benchmark their security.
- ATT&CK was created by MITRE to bring communities together to develop more effective cybersecurity.
- Available to any individual or organisation for use at no cost - open source.
- Used as a basis in the development of threat models and methodologies in government, the private sector, as well as the cybersecurity product and service community.
- Can be used at the elite level against advanced persistent threat groups APT.