NEED TO KNOW NEWSLETTER October 2021

Cybersecurity Awareness Month

Cyberattacks are speeding up

Organizations have been a driving force behind cybersecurity awareness and training. It's more important than ever to be up to date with cybersecurity knowledge so that attacks don't happen on your watch. For Cybersecurity Awareness Month you'll read about damaging attacks that happened in 2021 — and how employee actions changed the outcome.

Go slow and be suspicious!

An employee at Electronic Arts (EA) made a small but devastating mistake that caused harm to the company and allowed hackers to access their system.

Electronic Arts (EA) hack — Social engineering[1]

The EA hack started when a hacker purchased a stolen cookie (a small text file used to identify your computer as you use a network). This allowed them access to EA's Slack, a communication platform for organizations.

Once inside the organization's communication channel, the hackers pretended to be an employee who had lost their phone. **The IT department did not work slowly or take this communication as suspicious behavior.** Instead, they gave information to the hackers, and this information allowed the hackers to get into EA's system. Over 700GB of data was taken.

- EA stated that no player information was taken and there was no risk to player privacy.
- The hackers advertised game data for sale on underground forums. They stated that they would continue to leak information until they received a ransom.
- **What is social engineering?** Social engineering is when a hacker impersonates someone to gain access into an organization's system or even their physical space.

Verify and report!

Check out how employees of FireEye and SolarWinds responded to a hack ... and where a timely verification would have changed the outcome.

SolarWinds hack — Supply chain hack[2]

The SolarWinds hack was first spotted by someone at FireEye, a cybersecurity company. A staff member noticed that an employee signed in using their username and password but a new phone number.

This suspicious behavior set off alarms. The staff member needed to **verify** if the employee had a new phone number. In this case, they did not.

Once this was confirmed and they realized that an attack was underway, people jumped into action.

- SolarWinds is a software company. In this hack, network management software was compromised.
- Many large organizations such as Microsoft, Intel and even the US Department of Homeland Security were using SolarWinds. This meant their organizations were compromised, too.
- Sudhakar Ramakrishna, CEO of SolarWinds, immediately announced this issue to the world. He said, **"The right thing to do is report."**
- **What is a supply chain hack?** A supply chain hack is an attack on one part of a supply chain. This hack is efficient because it can get hackers into multiple organizations quickly.

For more information on the SolarWinds hack, check out the NPR Planet Money podcast *"One Hack to Fool Them All"*

Follow policies and procedures!

Here's a big one-- read about how one employee helped make a difference by taking quick action.

Colonial Pipeline attack — Ransomware[3]

A little before 5 a.m. on May 7th, 2021, an employee at the Colonial Pipeline noticed a ransom note on the computer, demanding cryptocurrency. This employee **followed the company's policies and procedures and immediately reported the situation.**

The Colonial Pipeline attack might be one of the largest and most impactful cyberattacks in history. It started when the hackers gained access to the Colonial Pipeline networks by using a leaked password to enter the company's VPN (virtual private network).

- **The VPN did not use multi-factor authentication,** a cybersecurity tool that adds an additional layer of protection.
- After extensive research, they found no evidence of a phishing attack. This led them to believe that the password used was the same password for another account that had been previously hacked.
- One of the country's largest pipelines was shut down, impacting gasoline accessibility and prices for about two weeks.
- **What is a ransomware attack?** A ransomware attack is when hackers gain access to an organization's system, encrypt and lock all of the data and then demand payment.

Contact Us:
www.etechcomputing.com
contact@etechcomputing.com
647-361-8191

Sources: 1 https://www.techtimes.com/articles/262969/20210716/electronic-arts-hack-stolen-data-now-being-leaked-vice-motherboard.htm 2 https://www.npr.org/2021/05/28/1001402799/one-hack-to-fool-them-all 3 https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password