SMALL BUSINESS CYBERSECURITY CASE STUDY SERIES

Case 5

NATIONAL CYBERSECURITY ALLIANCE

A Dark Web of Issues for A Small Government Contractor

SCENARIO:

The CEO of a government contracting firm was notified that an auction on the dark web was selling access to their firm's business data, which included access to their military clients database. The CEO rapidly established the data being 'sold' was obsolete, and not tied to any government agency clients. How did this happen? The firm identified that a senior employee had downloaded a malicious email attachment, thinking it was from a trusted source.

ATTACK:

A phishing attack where malware is in the attachment of the email.

A phishing attack is a form of social engineering by which cyber criminals attempt to trick individuals by creating and sending fake emails that appear to be from an authentic source, such as a business or colleague. The email might ask you to confirm personal account information such as a password or prompt you to open a malicious attachment that infects your computer with a virus or malware

RESPONSE:

The company's IT management immediately shut off communications to the affected server and took the system offline to run cybersecurity scans of the network and identify any additional breaches. The firm's leadership hired a reputable cybersecurity forensics firm. Each potentially impacted government agency was notified. The U.S. Secret Service assisted in the forensics investigation.

IMPACT:

The operational and financial impact from the breach was extensive – costing more than $1 million: The company was offline for several days disrupting business; new security software licenses and a new server had to be set up.

LESSONS LEARNED:

① You are never too small to be a target. A cyber attack can happen to anyone.
② Teach staff about the dangers of clicking on unsolicited email links and attachments and emphasize the need to stay alert for warning signs of fraudulent emails.
③ Install and regularly update anti-virus, network firewall, and information encryption tools to scan for and counteract viruses and harmful programs.
④ Conduct ongoing vulnerability testing and risk assessments on computer networks.

DISCUSS:

- Knowing how the firm responded, what would you have done differently?
- What are some steps you think the firm could have taken to prevent this incident?
- Is your business susceptible to this kind of attack? How are you going to reduce your risk?

RESOURCES:

- NIST Small Business Cybersecurity Corner: https://www.nist.gov/itl/smallbusinesscyber
- National Cybersecurity Alliance: https://staysafeonline.org/cybersecure-business/

This resource, funded through NIST Federal Award 70NANB19H165, is intended to be used for general education purposes. The content of the case studies is a combination of publicly available information, business-submitted information, and fictional details to create an educational scenario.