LBMC Information Security Cybersecurity Sense Podcast Show Notes
Author: Bill Dean
Episode: 22
Date: April 10, 2017

Phishing Emails With 100% Click Rate

Wombat Security Technologies Report—"2018 State of the Phish: Phishing Data, Insights, and Advice"

- The company based the report on data from tens of millions of simulated phishing attacks, and they found that:
  - 76% of organizations said they experienced phishing attacks in 2017.
  - Nearly half of InfoSec professionals said that the rate of attacks increased from 2016 to 2017.
  - The impacts of phishing were more broadly felt than in 2016, with an 80+% increase in reports of malware infections, account compromise, and data loss related to phishing attacks.
  - Personalized phishing tests (personalized email address, first name, or last name) are no more effective than non-personalized ones.
  - End users are most likely to report suspicious emails in the middle of the week.
  - The topics and themes that are most tempting to end users are "online shopping security updates," "corporate voicemail from an unknown caller," and "corporate email improvements."
  - Two simulated phishing templates had a near 100% click rate: one that masqueraded as a database password reset alert, and another that claimed to include an updated building evacuation plan.
  - Organizations in the telecommunications, retail, consumer goods, government, and hospitality industries have, on average, the worst click rate (15% to 13%), while those in the energy, finance, transportation and defense industrial base industries have the best (8% to 3%).
  - Average click rates fell across all four categories (corporate, commercial, cloud and consumer emails) this year in comparison to 2016.
  - The researchers particularly saw a significant improvement in click rates on cloud-based templates (business-related emails include messages about downloading documents from cloud storage services, or going to an online sharing service to create or edit a document).

- We have worked a lot of incidents that started with a similar phish.
- We have also seen a few DocuSign phishes that wreaked havoc.

FSecure Research Data

- Over one-third of all security incidents start with phishing emails or malicious attachments sent to company employees.
- Phishing and emails with malicious attachments together accounted for about 34% of breaches.

Key Takeaways

- We are all aware of how devastating phishing attacks are and that they are a key component in many of today's attacks.
- Training employees to spot phishing emails, messages, and pre-texting calls can't be done just one time or once a year if the organization wants to see click rates decrease.
    - For one thing, employees come and go (and change roles) with regularity.
    - Secondly, threats change over time.
    - Thirdly, knowledge and practices that aren't regularly reinforced will be lost.
    - And, finally, awareness isn't the same as knowledge.
- Notice that no industry reported a 0% click rate. That is the concern, attackers only need one user to follow the link in a phishing email and enter their credentials for your network to be compromised, just ask many of our clients.
- I will admit, with the 100% click rate on database password resets and evacuation plans, these approaches may be implemented into our many of phishing schemes.

References:

- https://www.wombatsecurity.com/blog/2018-state-of-the-phish-phishing-data-insights-and-advice
- https://www.helpnetsecurity.com/2018/02/23/weakest-link-security-perimeters/

Bill Dean is a Senior Manager at LBMC Information Security. While involved in various aspects of LBMC's security services, he is also the practice lead for the organization's incident response, forensics, and litigation support practice.