The Fallacy of the Protected Enterprise:

When Vendor Vulnerabilities Become Your Own

Clara Tsao
@tweetclarita

CYBERSECURITY EDUCATION SUMMIT
November 3rd 2017

Third party Risk

- **Critical Attack example**: Target (2013) , Yahoo (2014)
- **Open Source Example:** Heartbleed (2014)
- More and more attacks coming from third party vendors and weak “non-traditional” entry points
- “The path of least resistance into many organizations is through a third party that has been granted direct access to their environment,” T.R. Kane, Cybersecurity & Privacy Principal at PwC.

Weak Entry Point for Attack (*cyber paleontology*)

1. Weak Vulnerable Entry Point
Malware Infection (i.e. Email Phishing-malware)

2. Find second weak entry point
Gain Access via stolen credentials and/or exploit app vulnerability

3. Remain Undetected
Get name of targets and IP Info, Access tokens from domain admins, create new domain, propagate computers with new credentials

4. Share stolen information
Install Malware, and send stolen data (via network share and FTP)

Attack

- **63 percent of data breaches** were linked to a third-party vendor that was responsible for system support, development, and/or maintenance (Soha Systems Survey on Third Party Risk Management, 2016).
- In some cases, the victimized companies did not even know that a third party handled certain security functions.

Impact

“The average economic impact of a single data security incident was $720,000 in damages, and “one successful targeted attack could cost a company as much as $2.54 million.”

- Kaspersky Lab’s “IT Security Risks Survey 2014”

Too Much Trust?

- High level of trust in third-party vendors, but a low level of visibility of vendor access to IT systems
- 92 percent of respondents say they trust vendors completely or most of the time, although two-thirds (67 percent) admit they tend to trust vendors too much.
- Only 34 percent knew the number of log-ins to their network attributed to third-party vendors, and 69 percent admitted they had definitely or possibly suffered a security breach resulting from vendor access in the past year.

Mitigation

- Perform a Third-Party Vendor Assessment
- Write a Service-Level Agreement (3rd party must comply with company/organization’s security policy)

Affiliated: Mobile devices also seen as weak security point.

- Determining smart measures for smart devices

The Problem of People, Cybersecurity and Third Parties

1. Know your third parties
2. Know their business
3. Know their risk
4. Know their access

Additional security recommendations:

1. Multifactor authentication for remote access login
2. Include policies related to outdated operating systems and software in contracts w/ vendors
3. Ongoing employee security training

Additional Security Recommendations

Additional security recommendations:

1. Multifactor authentication for remote access login
2. Include policies related to outdated operating systems and software in contracts w/ vendors
3. Ongoing employee security training