Fraud Prevention for Small to Mid-Sized Companies

By Steve Jaffe – November 2018

Millions of phishing e-mails are sent daily. Hackers from foreign countries are tirelessly trying to find openings in networks to exploit companies for Bitcoin. While the larger companies, city networks and hospitals tend to make the news, it is typically the smaller companies that get hurt the most.

Network Fraud Prevention Strategies

Controls for your CFO/Bookkeeper

What to ask your Tech Provider

Mitigation thoughts should you be compromised

eDot, LLC

3075 Tollview Drive
Rolling Meadows, IL
60008

847 847 4500

www.eDotSolutions.com

edot℠
Providing solutions...
Managing your technology

If a hacker really wants to gain access to a network, they can. It's just how hard they want to try. The mantra at our company is to insist that every reasonable effort is made to ensure that the hacker just goes somewhere else. Too often, we have seen breaches due to carelessness and complacency. We have also seen the false expectations that Malware and Ransomware Licenses will block any possible intrusion. This article covers many of the basics and some of the more advanced techniques in blocking or mitigating an intrusion.

***

Assumption #1: A good hacker has the e-mail and password of someone in your company (maybe your administrator).
Assumption #2: A good hacker has your customer list, banks you work with and your vendor list.

Once you accept this, it makes it much easier to protect your company from bad people and bad acts.

***

While the overthrown Nigerian Prince is still alive and living somewhere, the techniques and methods to fraudulently take your money and shut down your network have gotten far more creative and sophisticated.

As a Managed Services Provider, we have seen a lot (all in the last 12 months)

- Clients sending ACH payments to Hackers (instead of their clients)
- Clients paying a hacker who is posing as a vendor.
- Clients wiring large sums of money to "partners" who turned out to be hackers in disguise.
- Spoof e-mails sent by hackers to look exactly like you asking you for money or change of address for payments.
- A compromised e-mail where the hacker hid rules to automatically forward all incoming e-mails to a private e-mail address (and then deleting all trace of this happening).
- E-mails apparently sent internally posing as an employee or owner when they weren't from those people asking to wire or transfer money.
- Clients leaving their Network "Door" wide open with weak and never changing passwords
- And of course, the 100+ variations of spoofing and phishing techniques.

***

The Basics of Fraud Prevention

Systems and Network

No, this is not everything. But, if you implement and are diligent about the points below, you increase your chances that the hacker will go somewhere else. You will need your Tech Company or your Network Administrator for some of these:

1. Ensure that you are protected with the four (4) basic Device Protections:
   a. A Malware AND Ransomware License on every Device and appropriate server
   b. Web Filtering installed, properly configured and managed.
   c. Spam Protection on every e-mail address.

   And, most important, ensure that your License Definitions and Versions are always current. You should NEVER opt for the Freeware versions.

2. Ensure that your Password Policies are thorough: Complex, 8+ characters, changed every 3 months (minimum), lockouts after 3 tries, and more. Do not allow ANY exceptions. We have seen policies implemented only to exclude certain people (typically owners who can't be inconvenienced).

3. Put in a dual/multi-factor password system for remote connectivity.

Don't be the Open Door.

4. Confirm you have NO open ports on your Firewall (s). Ensure that you are using a VPN (Virtual Private Network) or an RD Gateway for ALL remote connectivity. Confirm that there aren't any exceptions such as ones opened for Vendors.

5. Confirm FSRM (File System Resource Management) is configured properly and exceptions are managed. This is a fantastic tool to stop the spread of Ransomware, should it get into a device on the network.

6. Confirm Admin, System and Service Passwords are EXTREMELY complex and changed every 3-6 months.

7. Check your Active Directory monthly for removal of any non-employees.

8. Never share or keep lists of passwords (secured password programs may be an exception). Never send a password through e-mail (even internally).

9. Block access to all non-company e-mail sites for all employees (such as Yahoo, Gmail, etc.)

10. Install Geo Fencing on your Firewall and configure appropriately based on your business location.

11. Only have Admin rights on a workstation if absolutely necessary and you understand the risks.

12. If you do happen to click on a suspicious e-mail, but nothing seems to have happened, ALWAYS tell your Network Administrator. Don't delete the e-mail. Hold it for review.

13. Ensure you have an on-boarding and termination checklist that addresses any password/access issues including the disconnect and wiping of any mobile devices.

14. Consider engaging a company that specializes in Penetration Testing and/or Phishing Education for your employees.

Internal (CFO / Controller)

1. Never EVER send an ACH or Wire based strictly on an e-mail you received from ANYONE, including internal people or owners. ALWAYS confirm this information over the phone (or in person if internal) and only speak to someone who you know. Do not call the number ON the e-mail request.

2. Never change an address of any vendor based strictly on an e-mail. Always call the phone number you have on file (not a number in the e-mail) to confirm the address change.

3. Never change an ACH account number of any vendor based strictly on an e-mail. Always call the phone number you have on file (not a number in the e-mail) to confirm the ACH change.

4. If you receive a change of ACH information from a client where you do ACH pulls, ALWAYS verify with the client via telephone (from your client records), that it is approved and accurate. Strongly consider doing a test pull if a change is made.

5. Consider sending a mass e-mail to your clients telling them that "your company" will NEVER send a change of address, phone number or ach/payment change information via e-mail WITHOUT a request for you to verify via phone call.

6. Reconcile your bank statements as quickly as able (some controllers do it every day). Immediately report any suspicious debits OR credits. The person reconciling should not be the person who signs the checks.

7. If you receive a check from a client (or a refund from a vendor) where the amount or invoice references just don't seem to make sense, don't deposit it: Call the client/vendor first.

8. Check with your bank and accounting firm for any additional tips they may have for you.

Note: There are many other internal techniques that I am not addressing: dual check signatures, 2nd signature over certain amounts, check sequence audits, use of signature stamps, person reconciling can't be the person signing, who can add/change information in the Vender Master file, no single person can set up and send a wire (or ach), etc. These issues should be discussed with your bank or accountant.

Critical: Make sure you are properly insured with a Cyber and Fiduciary Insurance Policies should any of these events occur and you experience non-recoverable funds. Assume the worst.

***

About the Author

Steve Jaffe is the Co-Founder and active Partner of eDot, LLC a large Managed Services Provider located in the Chicago Area. Mr. Jaffe has a BS in Business Administration and a Master's Degree in Corporate Finance. He has been President and/or CFO of over a half dozen mid-sized companies in the previous 20 years. Mr. Jaffe, along with his business partner, Melvin Thoede, Jr. own a Managed Services Company, a Telecommunications Company, a Surveillance/Access Control Business, and a Web Development/Programming Agency.

Outside the office, Mr. Jaffe is a husband to a middle school teacher, father of four teenage children, a pilot, a chef, a writer and a voracious reader.

About eDot, LLC

eDot, LLC is a large Managed Services Provider (MSP) serving businesses and school districts with 1 to 500 employees in the Midwest and throughout the United States. For information on our services or for more information on our Client Security Programs/Audits, go to www.eDotSolutions.com for complete contact information.