How an E-Mail can do so much DAMAGE

There is a very common scam going on right now and it involves a compromised e-mail account; either your company's e-mail or your vendor/ customer's e-mail. We call it the ACH scam, but it can happen in many different ways. Here's the breakdown.

Volume 24, Issue 7
July 2024

1. The most common way they gain access is an employee who gets tricked into giving their e-mail credentials to a hacker.
Example: The employee gets an email that says "Someone shared a document with you. Click here to open it." etc.

2. But there are many other examples of how an account can be compromised.
Once the hacker gets access to this e-mail account, he looks everything over for days, trying to figure out what that employee does, who they pay or who they expect to get payment from.

3. The hacker then e-mails (as if they are your employee) a customer of yours who owes you money. They are informed that your bank account was changed and that they need to send their payment to this new ACH or bank account.

4. Customer takes the money they were going to pay YOU and instead pay the hackers. After all, the e-mail did come from one of your people so it must be legitimate, right?

5. When your company does not see payment after a couple months, you reach out to your customer to find out why and they tell you they have already paid. But it's not in your bank account, it's in the hacker's.

6. You then determine an account was compromised on your end. You let the customer know this and that they still owe you money. They disagree. They said they have already paid the bill once; they aren't going to pay it again. After all, it's an issue with YOUR e-mail, and it's not their problem.

7. You are out (possibly) tens of thousands of dollars.

Sound unlikely? It is currently happening all over the place, and it has resulted in big losses for companies who do not follow proper security practices. So, what can be done?

Continued on Page 2

...Continued

1. TRAIN YOUR PEOPLE – Aeros offers training on best practices, and we have online or onsite in-person options for training as well. A good example of training would be to make sure that none of your employees clicks on ANY link, no matter who it comes from, and that the user NEVER sends their username, password and MFA if they are not 100% sure of where it is coming from. We can help show them how to avoid this pitfall.

2. CREATE POLICIES – Perhaps, to protect yourself, you could send an e-mail to all customers explaining that you will never send them a change in your bank account or ACH without a phone call and never solely through e-mail. Also, for internal financial changes, let your people know that unless they hear a "password" from one another, no changes will be made unless the other employee or supervisor uses this verbal password. Again, this would be done over the phone, not through e-mail!

3. SECURITY – Make sure all passwords for e-mail are at least 12 characters long, make sure the passwords get changed on a schedule and that every account has a valid and activated MFA method (like using your cell phone or USB security key.) If you have our office 365 services with advanced security, we are usually the first ones to be aware of a compromised account that is either being accessed outside the country or we see that MFA methods are being added to the account or that new rules are being created in Outlook to hide the hacker's communication.

GMAIL: Is your company on Google Docs and use Gmail for your correspondence? Unless you stay on top of your security preferences in Gmail, you may be susceptible to these attacks with no way of monitoring or being clued in on a potential breach. Give us a call, and we can assist with bumping up your Gmail security by adding some capabilities to your existing Gmail services or even migrating your business to Office 365.

The point is, if your employee decides to accidentally supply a hacker with their username and password – **EVEN IF THEY USE MFA** – their account may already be compromised without your knowledge! It would be only a matter of time before the hacker comes up with a game plan to get money from you or your customer. Plus, your reputation could suffer.

Avoid these pitfalls. Get with Aeros if you haven't already had us harden your e-mail accounts and bumped up security on them. Ask us about our B2K training/dark web/phishing simulation services that help you get control over all of your employee's actions.

Or if you have not had an assessment recently, have us come onsite to explain. It is at no cost to you, and we perform the assessment at your location.

Building Relationships in West Michigan since 1976!

Aeros

A DIFFERENT WAY TO I.T.

Aeros IT Group

6261 Lake Michigan Drive
Allendale, MI 49401

Phone: 616-997-8324
Email: support@aerosgroup.com

FIND US ON THE WEB!
AEROSGROUP.COM