INFO ADVANTAGE

Can You Withstand A Cyber Attack?

Imagine the embarrassment of having to notify your clients and vendors that, **because of you, their information may now also be in the hands of cybercriminals**; paying pricey emergency IT fees while your operations are halted or severely limited for days or weeks, data loss, lost clients, potential lawsuits or government fines for violating data-breach laws. Your bank account drained, with no bank protection.

It doesn't have to be that way.

Discover how to secure yourself and your data with a penetration test.

Learn how easy it is for hackers to get to your information if you're not keeping track of it. Make sure your team is adhering to good cyber hygiene.

Nearly every data breach is preventable.

Unfortunately, cybercriminals rely on the common belief that just because you've been able to avoid an incident like this in the past, you're safe now.

How the penetration test works:

1. **Click on an executable**
   (simulating what happens when a link in an email is clicked).
2. **Run the executable once**
   This takes between 5 minutes and an hour (up to 2.5 hours on older machines). **Go about your normal routine as it runs**.
3. **We will analyze your results**
   and present our findings as to **what a hacker would find on your network**. This will include cloud drives, One Drive, DropBox, Box, SharePoint and other file-sharing programs.

What we will analyze:

- **Security Patches & Vulnerability Management**
- Discover whether your network has vulnerabilities resulting from **patch management issues**.
- Test Your **Network Perimeter Defense**
- Our scanner will test **whether your firewalls are configured correctly** and report issues if they did not appropriately alarm. Using multilayered boundaries, including a firewall, Intrusion Prevention and Intrusion Detection are more critical today than ever before.
- Test Your **Identity & Access Management**
- Learn if **your team is using stale, repeated or crackable passwords** for accounts on your network. Security best practices for handling passwords and credentials are employed, such as the usage of multi-factor authentication for remote access, critical accounts and administrative accounts, enforcement of a strong password policy, absence of default and/or shared accounts, etc.
- **Identify Serious Data Leaks**
- Determine **where sensitive data is stored** on your devices and make sure it's being guarded. Hackers commonly exploit both your network and data assets when attacking your network.
- **Determine Your Malware Defenses**
- Find out if you have an **appropriate cyber stack** that will respond to a virus attack.
- Get The Information To **Inform Your Cybersecurity Decision Making**
- **Gauge where your cybersecurity is today**. Learn whether data encryption, along with information about what a hacker can see around an infected device. Determine if your network would withstand an attack (even on one machine!).

SalesReq@info-adv.com | (585) 254-8710 | www.info-adv.com