Online Threat

Growing Risks of Benefits, Payroll Platforms

THERE IS a growing threat to companies that use online services to administer their employee benefits and payroll as cyber criminals increasingly exploit these cloud service platforms.

The results of a hacker gaining access to the company's payroll systems, sloshing with cash, as well as employees' personally identifiable information can be devastating both to the employer as well as its workers, according to a blog by the law firm McLane Middleton.

Do not assume that the system you are using has safeguards in place to prevent these types of attacks. Sometimes you may need to activate them on your account or configure your account a certain way.

PLATFORM VULNERABILITIES

Cyber criminals can gain access to sensitive employee information:

- Social Security numbers
- Government identifications and numbers
- Bank account information for employees and dependents
- Health information

Cyber criminals may gain access to funds that go throughr:

- Payroll
- 401(k) and other retirement accounts
- Health insurance
- Other benefits

Attacks on online benefits and payroll services can result in huge losses as well as liabilities for an employer. Damage can be extensive:

- The criminals can divert large financial transactions like payments to retirement funds and smaller ones like payroll payments, to a fraudulent account, which they promptly drain.
- The criminals steal personal information of employees. They can then demand the employer pay a ransom in exchange for not selling the information on the dark web. If the employer refuses to pay, they can demand individual employees pay a ransom.

What you can do

Often hackers will gain entry to a benefits and payroll website not through any fault of your own.

McLane Middleton recommends that you look for online benefits and payroll platforms that protect their clients' accounts with:

Multi-factor authentication – Besides a password, a platform worth its salt will include multi-factor authentication. Typically, that entails sending an authentication message to a pre-specified e-mail or mobile phone number that can accept text messages every time there is a log-in attempt.

Other systems may use certificates that the employer installs only on computers used by employees authorized to access the platforms.

Multi-user notification and authorization – This entails notifying key personnel if an employee's profile information (such as physical address, phone number or bank account number) is changed inside the payroll or benefit system. The website would then send an e-mail to a secondary person in the organization to approve the change.

Different levels of access privileges – One common approach is for hackers to target employees in an organization with administrator access to the benefits and payroll system. All of the employees that use the system often do not need access to all of it.

You can limit access of your human resources staff to only those functions necessary for them to do their jobs. This prevents them from accessing files and information they have no business seeing.

Logs of access and activity – If possible, try to find a vendor that saves log files that can record dates and times of a breach, what the criminals were doing in the system and what data they accessed.

The takeaway

If you are using an online platform to administer your benefits and payroll, you should ensure that the vendor is taking the appropriate steps to protect itself, and you, from cyber attacks.

You may want to discuss with your vendor what kind of security they have in place and any extra steps you can take as an organization to reduce the chances that information and funds in your accounts are safe from abuse. ❖