Could HR Be the Next Target?

Marshal your organization's defenses to prevent cyberattacks.

By Drew Robb

Could HR departments become a battleground reminiscent of the HBO series "Game of Thrones"? Instead of bloody skirmishes, HR professionals would face system attacks through hacking and phishing. Well-publicized breaches at CareerBuilder and Monster could mark the beginning of a long war over tech security.

"Imagine the power of the HR system: It has full names, dates of birth, Social Security numbers, pay rates, employee bonuses and annual reviews," says Chris Hadnagy, CEO of Social-Engineer Inc. and author of *Social Engineering: The Art of Human Hacking* (Wiley, 2010). "It holds all the keys to the kingdom for the company."

So how can one keep the HR realm secure?

Greatest Threats

Hollywood often portrays hackers as lonely guys working out of their basements. But, in reality, the greatest threat often comes from organized, well-financed groups that use technical and social skills to take over entire computer systems. While anti-virus software and firewalls protect HR information systems (HRIS) from broad-scale attacks, they leave information vulnerable to the most prevalent danger, which relies on human rather than system weaknesses. Generally known as "phishing," these latter types of attacks occur when an impersonator convinces people to give up secure information under false pretenses.

For example, in 2009 hackers acquired files relating to Coca-Cola Co.'s $2.4 billion agreement to buy China's largest juice vendor. At that time, Coca-Cola executives were promoting ways to reduce the company's consumption of energy. In February, an executive involved in the negotiations received an e-mail about saving energy that appeared to be coming from another executive. He clicked on a link purporting to be a message from the CEO; doing so installed malware that gave hackers access to his computer.

The next month, the criminals also gained entry into the computer of a Coca-Cola public affairs executive in China, who received what seemed to be a PDF containing a media advisory from the World Bank's office in Beijing. With these computers compromised, the thieves could gain broader access to the company's network and steal documents relating to the proposed purchase, which then fell through.

HR Beware

Given the personal data to which HR has access, it's not surprising that HRIS has become a key target.

"Cybercriminals are skilled at adding phantom employees to payroll, including them in 'direct deposit' lists and having a money mule waiting at the bank for a payroll deposit to the phantom employee," says Stu Sjouwerman, founder and CEO of security software and training firm KnowBe4 LLC.

One method of attack that has surfaced this year is the use of Trojan software called Gameover ZeuS. This software has been used for several years to illicitly gather banking information, and some hackers have started using it to target HR departments that use CareerBuilder or Monster for recruiting.

The attack comes in two phases. Step one is a phishing attack that enables hackers to access a workstation and install Gameover ZeuS. The malware captures vital usernames and

passwords and sends the information to the hackers.

"HR staff has a tendency to be helpful, and that can make it an even bigger target," Sjouwerman says.

Step two involves tricking an employee into giving additional information that is needed to take full control of his or her organization's CareerBuilder or Monster account. This can involve creating fake security questions that look identical to the ones used by the recruitment sites and capturing the employee's answers.

"If the account is tied to a bank account and has a spending budget, it can become a target for banking Trojans," Sjouwerman says.

Security expert Brian Krebs recently exposed another attack that involved capturing login information for payroll and HR management provider UltiPro. The hackers downloaded employees' W-2 information and even filed fake tax returns using H&R Block's e-filing service. The fraudulent refunds were automatically loaded onto prepaid American Express cards that were mailed to drop sites around the country and cashed.

Gone Phishing

Some of the most dangerous cyberattacks are based on social engineering—the exploitation of human rather than IT system weaknesses as part of a complex fraud scheme. Common forms include:

Phishing. A person receives an e-mail that purports to be from a legitimate source, such as a bank, and is asked to provide his or her account number and password.

Vishing, or "voice phishing." A hacker calls targets to obtain desired information. Common examples would be someone pretending to be a "tech support specialist" calling to verify an employee's password or an HR person calling to confirm direct deposit information.

Spear phishing. A particular individual or organization, rather than a broader group, is targeted.

Low-Tech Protection

Not all HR security threats are so sophisticated. At one company, an HR employee was working on his laptop at a Starbucks that had a secure connection into the HR system. But when he got up and left the laptop unattended, someone gained access to all the HR records at his company.

A simple change in policy helped prevent future breaches: The company began training its employees not to leave their laptops unattended.

"The problem was not solved from a technical point of view, but from a policy point of view," says Humayun Zafar, assistant professor of information security and assurance at Kennesaw State University in Georgia and author of the security chapter in the textbook *Human Resource Information Systems* (Human Resource Management Review, 2013). "Information security is 20 percent technical and 80 percent managerial."

Hadnagy knows of another company that had retained a casual atmosphere even after its revenue had grown to the tens of millions. After the company let an employee go, they allowed him to make an unsupervised visit to clean out his office after other employees had left for the day. The next morning, they found that all the servers and backup disks had been erased and reformatted; they couldn't prove he was the one who did it because all the log files had been wiped.

"Fortunately, they had an offsite backup that was two months old, but they still lost two months' worth of their accounting, orders and processing data," Hadnagy says. "The amount of time and effort it took to bring that back was astronomical."

Once again, the solution came down to policy—in this case, implementing a security protocol dictating that when someone is fired, HR immediately disconnects his or her network accounts and revokes access to the building.

Raising Awareness

Experts recommend the following steps to keep HR data secure:

Set the security protocols of cloud services to make data private. This also applies to any files stored on local servers that can be accessed through the Web.

"Your own corporate servers may be secure, but if you are uploading files to a www directory, Google will cache it and hackers will find it," Hadnagy says. ›

Securing Windows XP

Windows XP has had a long run as far as PC operating systems go. Most software gets replaced every few years, but XP, released in 2001, was still running on nearly 28 percent of desktop computers in March 2014, according to Web analytics company Net Applications. It was on more systems than Windows 8, Windows 8.1, Windows Vista, Mac OS X and Linux combined.

For now, most anti-virus vendors will continue to support XP for at least two more years, which will guard against certain malware. But the unpatched vulnerabilities could compromise an entire network. This came to the forefront in April 2014 when a flaw was discovered in all versions of Internet Explorer that could allow hackers to take control of a user's computer.

"I found a file the other day that had the phone numbers, e-mail addresses, physical addresses, Social Security numbers, dates of birth and full names" for a company's employees.

Review HR security procedures periodically. Companies should beef up their security if they engage in cloud computing, allow employees to bring their own devices or collect "big data." "Those three things by themselves are huge, but in HRIS they all come together," Zafar says.

Test and train employees. Fortunately, the best defense is something that HR is already adept at doing: training and testing. Testing might involve sending employees simulated phishing e-mails and educating them if they respond. For training, try sending a weekly security tip to all employees and give new employees security awareness training as part of the onboarding process. Everyone, especially HR employees, should receive routine refresher trainings.

What doesn't work, Sjouwerman says, is training employees once a year "in what we call 'checkbox compliance'—break room sessions with coffee and doughnuts, showing them 10 slides, telling them not to click on bad links, and expecting them to remember that for another 12 months."

After all, the stakes are high: HR systems are a treasure trove—a primary access point to your employees' vital information. And, as anyone who watches "Game of Thrones" knows, whoever holds the keys to the kingdom needs to watch their back. Make sure there's not a target on yours. HR

WEB EXTRAS

For links to more information about cybersecurity, including a video that offers tips for protecting HR data on company networks, see the online version of this article at www.shrm.org/0714-technology-security.

Drew Robb is a freelance writer based in the Los Angeles area.