TECHNOLOGY

Protect against human nature

Staff can pose a big risk to computer network security, however inadvertently. *Andrew Don* explains how to use technology to keep data and business reputation secure

When we think of computer security, most of us think of viruses, malware, spyware and hacking. Many blame the operating system and software for security holes that criminals can exploit. We rarely think it is our fault.

Yet the vault of system horrors needs help to invade and these can often manifest in the weaknesses of business bosses and their staff.

Oz Alashe, chief executive of GCHQ-accredited cyber security platform CybSafe, points out that security researchers at IBM and the Cyber Security Intelligence Index have found that 95% of successful hack attacks or incidents happened because of some type of human error.

This is where Identity Access Management (IAM) – controlling who in your company has access to what – makes all the difference.

Role-appropriate privileges

Handd Business Solutions, an independent specialist in global data security, recently produced a report stating that proper access management requires users to have different system privileges depending on their roles and responsibilities.

It goes on to say that electronic crooks use cyberspace to probe company networks, testing for weaknesses thousands of times each second.

Cyber security experts say most weaknesses that criminals exploit are human ones.

These include: lack of personal discipline among computer users; failure of those responsible to manually install software and update operating system security in a timely fashion; or failing to automate the process.

It also encompasses the stress, trust, or lack of care or training that persuades staff to click on hypertext links that unleash ransomware, keyloggers or other nasties.

Phishing attempts might cause accountancy staff to inadvertently input bank account passwords into fake websites designed to steal credentials, for example.

Alternatively, staff with numerous passwords write them on sticky notes – in view of everyone.

The risk increases if all staff have access to every part of the business systems. This is why IAM is crucial.

Least-privilege access ensures that juniors only see the data they need to and can only manipulate that data accordingly.

Disgruntled employees or ex-employees might steal sensitive data, or some users might inadvertently put the company at risk by sharing information and passwords with people they should not.

Staying alert

Paranoia is the best policy, security experts say when it comes to safeguarding systems.

Businesses of all sizes are at risk. Adrian Cohen, managing director of Israel Travel Service (ITS) a small tour operator that specialises in pilgrimages to Israel, used to think he was too small to worry.

When he received an email claiming to be from Palestinian terrorist organisation Hamas,

"Cyber security research shows that antivirus software alone just isn't enough"

Oz Alashe, CybSafe

Abigail Healy
020 3714 4111
ahealy@ttgmedia.com

Abra Dunsby
020 3714 4112
adunsby@ttgmedia.com

Andrew Doherty
020 3405 6526
adoherty@ttgmedia.com

warning that he should not send anyone to Israel because the group was threatening imminent terrorist action, he initially wondered how it found him.

Yet the answer is, quite easily. He pays for Google AdWords so his company appears on the first page of Google when you search for: "Book a pilgrimage to Israel".

ITS uses online platform Concorde for various business functions, such as preparing invoices, receipts and creating a diary and reminders.

Cohen says: "On Concorde there are varying levels of access and I have the highest."

However, even the most savvy can fall victim to phishing attempts. Cohen recalls how his business received an email requesting a ticket to Tel Aviv. The "customer" paid by credit card and was issued the ticket.

"On the day of departure we were advised he was a no-show. We then got notification from the credit card company that it was a stolen card. He came back and requested a first-class ticket to Lagos for him, his mother and his sister.

"What he tried to do was set us up by getting in touch and pretending to be legitimate, then going for the big kill. It was all done by email. We get so many of these emails that are so obviously fraud. You can tell by the English, or the email address gives it away."

Costly errors can be avoided with staff awareness campaigns. Tui, for example, says it continues to invest in the enhancement of the security of its IT systems and developing internal awareness campaigns to help staff behave securely online.

Effects for all

Danny Maher, business solutions chief technology officer at Handd, says everyone needs safeguards whether an individual homeworker, a small start-up agency or a multinational enterprise.

Cyber security expert Alan Woodward, visiting professor at the University of Surrey, says not everyone in a business would be given authority to sign a cheque. The same should apply to many other processes - most of which are now online.

CybSafe's Alashe adds: "Cybersecurity research consistently shows that antivirus software alone just isn't enough. In a cyber landscape dominated by a mixture of social engineering and technological attacks, only strategies that bring into play human as well as technological defences, will offer genuine security."

IAM pointers

- Store data on a private server if you store it in-house.
- Data should be accessible on a need-to-know basis.
- IAM manages users' logins, ensuring only those with the right credentials can get in.
- Modern access systems should use two-factor authentication to make security more robust.
- An IAM system will use the concept of least privilege. This means an IAM system might only give junior sales executives access to the names and numbers of customers to which they have been assigned, while granting more senior staff access to the entire database.
- User behaviour analytics (UBA) will alert managers to unusual activity that falls outside a person's regular behaviour patterns. If an employee who only accesses company records from a single computer during office hours suddenly tries to download files from another device outside the organisation in the middle of the night, a UBA tool will notice.
- Use "information rights management", a data protection mechanism that uses pre-defined policies to control access to data on a per-document basis.

Source: HANDD