

6 April 2011 Last updated at 02:24

214 Share f t e

Tracking the internal threats

By Mark Ward

Technology correspondent, BBC News

Whistle-blowing website Wikileaks does not just spell trouble for the US government, Bank Julius Baer and the other companies, organisations and individuals that feature on the site.

Its mere existence and the appearance of many copycat sites is starting to occupy the minds of those who oversee security in every large company.

Why?

"Simple," said Philippe Courtot, founder and chief executive of security firm Qualys, "because every company has something to hide."

In most cases, he said, those secrets are just details of deals that are about to be signed, products under development or strategy changes. But also, he said, many firms have "dirty laundry" that would damage their reputation if it became public.

Wikileaks is tricky to defend against, said Mr Courtot, because the threat it poses is very diffuse and it comes from the inside. Before now, he said, corporates have put most of their time and money into defending themselves against external attack.

Spam filters, firewalls, anti-virus programs and intrusion detection systems are all about stopping the bad guys getting in. This makes sense because there are many millions of malicious programs and legions of cyber thieves endlessly trying to subvert employees and networks for profit.

Attack profile

Those defences are not entirely useless against the threats that Wikileaks pose, said Alex De Joode, security officer at hosting firm LeaseWeb.

They can come into play if supporters of Wikileaks take action in its name.

"What Wikileaks does is not really cyber crime," said Mr De Joode, "The acts of the individuals who tried to make companies accountable for their actions against Wikileaks using denial of service attacks, that's cyber crime."

In Operation Payback, many Wikileaks supporters joined forces to bombard well-known web firms such as Paypal, Amazon and Visa with data in an attempt to knock them offline. The targets were chosen because the firms, in the eyes of those supporters, had not done enough to support Wikileaks.

At such times, said Mr De Joode, established defences work because they are designed to defend against precisely those types of attack.

Not all defences point outwards. Inside corporate networks there are also tools available to watch what employees are doing.

Mohan Koo, managing director of security firm Dtex, said it was possible to monitor every mouse click and key press employees make, no matter the size of the company.

"But," he said, "no-one is going to do that because there's just too much data."

Equally wrong-headed, he said, was for a company worried by Wikileaks to clamp down on what their employees do online.

"A company might think they have locked it down and there's nothing going on," he said. "but all they have done is make people look for ways around the blocks."



Wikileaks has got many companies thinking about how to monitor data movements

Related Stories

[Wikileaks 'helped Arab uprisings'](#)

[Anonymous publishes bank e-mails](#)

[India vote 'influenced by cash'](#)

Top Stories



[Nato leaders: 'Gaddafi must go'](#)

[Phone hacking test cases approved **NEW**](#)

[Croats convicted of war crimes](#)

[Typhoon jets grounded over spares](#)

[Royal wedding details announced](#)



Security systems can defend against attacks carried out by Wikileaks supporters

The statistics gathered by strict intranet monitoring tools might suggest that nothing nefarious was going on, he said.

In reality, security was likely to be compromised more because employees are using subterfuge to do the things they are used to doing, such as updating Facebook, while at work.

Having an unmonitored channel over which company information is flowing is a real problem, he said, given the increasing need to gather data to satisfy industry regulations; the scrutiny of bodies such as the Information Commissioner and the potential damage a brand would suffer in the wake of a leak.

Even worse, he said, a crackdown on web use during work hours might dissolve the bond of trust that should exist between a worker and their employer.

That relationship would suffer, said Mr Koo, if firms use technology in an adversarial manner.

Trusting times

Far better, he said, was to show employees why security matters to their personal lives as well as in the workplace.

"Remind them that security is about looking after their interests as well as those of the company," he said.

"A lot of users and employees are not aware of the implications of their day-to-day actions," he said.

Showing how unprotected phones, laptops or desktops could lead to lost data would help them at home and at work, he said.

"The whole objective here is to build trust," he said. "You need to get those employees to buy into the reasons you are doing this."

More trust, he said, meant a workforce that was less likely to leak or feel motivated to expose internal secrets.

One radical way to avoid the risk of having secrets exposed is to have no internal secrets.

Indian technology firm HCL took this approach as part of a re-working of the company that began in 2005.

The need for change was driven by the realisation that although the company was still growing, the market for outsourcing was growing faster and it was getting left behind.



Good habits can help keep data safe at home and at work

At the heart of the change, said HCL director Bindi Bhullar, was the decision to put employees, rather than their managers, in charge of the business.

"Those that understand the business the best are the employees," he said. "The value for the company is created between employees and customers."

Managers at HCL now work to ensure that employees get the support they need to do their job better. Part of that, said Mr Bhullar, involved sharing information about how the company is organised, details of employee reviews, who gets paid what and details of contracts and customer contacts.

"Internally we share a lot of sensitive data," he said, adding that the approach has not been without its problems.

But, he added, sharing that information, sent a strong signal about how much the company trusted its employees and helps to get them more engaged.

"If someone is engaged then you are going to lower the risk of someone blowing the whistle," he said. "Trust and transparency insulate you from issues like leaks."