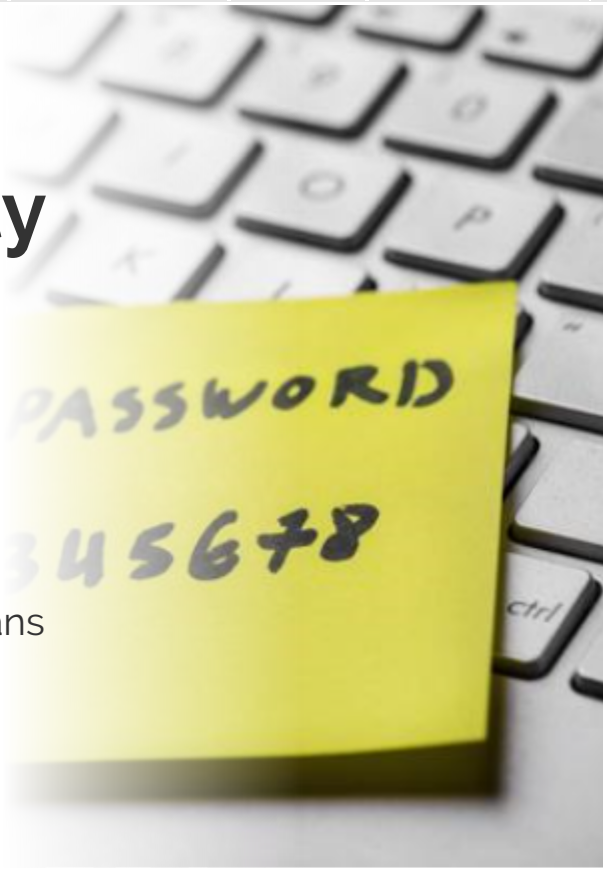
Security: 'Sticky note' vulnerability still bringing organisations undone



Security in Depth confirms that humans remain organisations' key weakness

Rohan Pearce (Computerworld)
15 October, 2018 12:14

Call it the sticky-note hole: As information security vulnerabilities go, it is low tech but profoundly dangerous nonetheless.

And in the case of organisations that are suppliers to some of Australia's highest-profile enterprises, including

major financial institutions, the consequences of employees scribbling down passwords on a piece of paper are potentially devastating.

The chief executive of Security in Depth, Michael Connory, said that while Australian businesses have been focused on protecting data "they tend to leave their front door open — they tend to forget about their staff".

Earlier this year Security in Depth launched what the CEO described as a "cyber credit score": The Cyber Assurance Risk Rating (CARR) is audit service that helps organisations asses the risk represented by a particular supplier.

The service provides the company's clients with an indication of the relative security maturity of a supplier, allowing an organisation to take steps to mitigate any associated cyber risks.

Since its launch, about 130 supplier organisations have been assessed as part of CARR, Connory said, with the process effectively functioning as an in-depth survey of where Australian

Editor's Recommendations


Apple pushes back against 'dangerously ambiguous' encryption bill


NT government plans $1m boost to IT industry


Labor's Rowland warns against rushing encryption bill


Scaling up FTTC to be NBN Co's next big challenge, CEO says


Private equity firm eyes possible MYOB acquisition


Telstra priority assistance service faces scrutiny

Web Events

businesses are making security missteps.

"We sat down, for example, with one financial organisation that is managing hundreds of millions of dollars of people's finances," the CEO told *Computerworld*.

"They'd encrypted the files, they had two-factor authentication. It was really quite good to see that they're utilising technology. [But] when we had a simple walk around their office, we found passwords located on desks. We discovered that when people were trying to phish them there was no real process for managing an attack — the best practice, they thought, was just delete it and not tell anybody."

In a case of cyber serendipity, through the CARR process Security in Depth found that a business email compromise attack was taking place at one of the organisations it was auditing.

READ MORE
Cyber security centres warn of RATs, 'katz

"No-one had seen it," Connory said. "We discovered that the CEO's email

Latest Jobs

IT Technical Support Level 1 & 2

people2people
Homebush NSW 2140
$25 - $30
Read more

IT Project Manager

MPAU Technology
Sydney NSW
Read more

Trainee Recruitment Consultant - IT

had been spoofed, and that the spoofed email addressed was communicating successfully with the CFO without the CFO recognising that it wasn't the CEO."

Connory said that a key failing that CARR has helped unearth is that organisation lack an overarching security framework to guide their efforts.

In the case of the organisation in the middle of a business email compromise attack, Security in Depth "sat down and said, 'Okay you've got policies and procedures in place – how did you come up with these policies and procedures?'" the CEO said

"They said, 'Oh when anybody ever asks us for a policy or a process around a particular security area, what we do is we develop it."

READ MORE

Apple pushes back against 'dangerously ambiguous' encryption bill

"So it's an ad hoc approach," Connory said. "They might be asked, 'Okay, what is your incident response plan'

Related Whitepapers

and they'll create an incident response plan to satisfy that particular requirement. Or 'how do you manage data at rest' – they'll come up with a plan at that point of time."

One of the key findings from the process is that many organisations still have no concept of how to detect whether they have suffered a breach, he said.

Another is that security awareness training remains minimal in many organisations.

"Eighty per cent of the organisations that we're talking to haven't seriously covered off cyber security training – they've talked about 'you need to be safe with information, you need to be safe with your browsing, don't clock on an email that you don't know'," Connory said. "That's the level of training that staff are getting."

READ MORE

Government encryption bill: Cisco, Mozilla join chorus of tech critics

There's often no concept of password management, for example, he added. One organisation, which manages more than $350 million on behalf of

clients, had stored 300 passwords for major applications in a Word document, he said.

Despite it being a confronting process, organisations are generally reacting "positively," he added.

"I think they're very realistic about where they're at, but they understand that there are significant issues." For larger organisations, Security in Depth has been pushing for the adoption of the US-developed NIST framework. Smaller organisations should at the very least be looking at implementing the ASD's Essential Eight, Connory said.

Membership is free, and your security and privacy remain protected. View our privacy policy before signing up.

Tags social engineering cyber security Security in Depth security

More about Assurance Australia

0 Comments

Read next

NBN Co says less than 4 per cent of fixed wireless cells ...

Cyber security centres warn of RATs, 'katz

DMARC adoption: Three in five ASX100 companies at risk of email fraud

Inside Investa's new Sydney HQ, designed around 'open, transparent and collaborative' culture

In pictures: Google opens new Melbourne office

Micron plans US$100 million AI investment splurge

US chipmaker says a fifth of its venture capital funding for startups will go to outfits led by women and other underrepresented groups