The [redacted] security war: How affe[redacted]

Pead PR, 2019

Monday, 25 November 2019, 8:51 am
Press Release: Pead PR

25 November 2019
The cyber security war: How New Zealand businesses are affected
New research on cyber threats facing New Zealand organisations

- **More than a third of NZ businesses have been hacked in the past year.**
- **42 percent of businesses expect their company will be hacked in the next year.**
- **20 percent of businesses said they would pay a ransom between $10,000 – $20,000 to retrieve stolen data. Almost one in 10 would pay more than $50,000.**
- **One in three Kiwi businesses haven't assessed the impact a hack would have on their company.**
- **Only half of businesses are aware of impending New Zealand Privacy Bill changes involving mandatory breach notification.**

Research released by Aura Information Security shows New Zealand businesses are feeling the wrath of cybercriminals with more than one third experiencing a cyber-attack in the past 12 months, a 10-percentage point increase on last year.

Kiwi businesses believe the situation is only going to get worse with 42 percent expecting their company to fall victim to a cyber-attack in the year ahead.

These statistics have emerged from a survey which polled more than 360 IT decision makers on their experiences of cyber issues in their business, ranging from SMEs to large corporates, right across New Zealand.

Aura Information Security General Manager, Peter Bailey, says business has never been better for cybercriminals.

9

"Sadly, cybercrime does pay – and it pays well. Hackers have an ever-expanding skillset and it's getting easier for them to find weaknesses in business networks and staff emails that allows them to gain access to large quantities of personal and financial data."

The prevalence of advanced ransomware is funding hackers across the world, and it highlights the value of data. While almost 40 percent of respondents would not pay a ransom, 20 percent of Kiwi businesses said they would be prepared to hand over between $10,000 and $20,000 to regain access to their data if it was locked or stolen. Almost one in 10 businesses would fork out more than $50,000 if faced with a ransomware attack.

"Intelligent automation means most attacks these days start with little human involvement. These probes run around the clock and only alert the hacker once a weakness is identified. That makes cyber-attacks highly efficient, as the hacker only need focus on 'qualified leads', when their malware has already made its way into your systems," says Bailey.

With the increase in automated malware, there should also be an increase in businesses undertaking regular penetration testing notes Bailey. Unfortunately, this isn't the case, with less than half of Kiwi businesses undergoing system penetration testing in the last year.

"Penetration testing is vital to ensuring secure systems. It allows businesses to patch holes in weak areas and help to prevent hackers from gaining access. Without that, your business can be open to a security breach."

Bailey confirms the threat of a breach is always present.

"Cybercrime is a constant fact of our modern life. Your technology is being probed all the time and you may very well experience an attack. All it takes is a moment's inattention, a single unsecured machine or uninformed employee, and even the best of defences can be compromised.

"Cyber security is only as strong as the weakest link, but with the majority of organisations not understanding current password best practice, we're not off to a great start."

Privacy Bill updates will take some businesses by surprise

Bailey was surprised to find that only half of Kiwi businesses are aware of the impending Privacy Bill changes on mandatory data breach notification.

"This is an alarming statistic considering 20 percent of businesses are not prepared to notify customers in the event of a security breach, despite the fact they will soon be legally required to do so. What's even more concerning is this number is up from 17 percent in 2018.

"Another worry is that almost a third of New Zealand businesses are not assessing the impact a significant breach would have on their organisation. Not only are these organisations putting their head in the sand, they could also face some hefty fines if they are introduced as part of the changes to the Privacy Bill," says Bailey.

More than half of respondents said the prospect of large legal fines would lead them to review their cyber security protocols.

"With the implementation of similar legislation in Europe and Australia over the past few years, we are just starting to see the positive impact this can have. As the proposed fine regimes for New Zealand are significantly lower compared to other countries, it will be a waiting game to see whether this change has a significant impact or is enough of a deterrent for businesses.

"When it's all said and done, money talks. I'd love to see the introduction of fines be included in the Privacy Bill updates in 2020," Bailey notes.

Head in the clouds

The report also revealed an unfounded sense of trust in cloud storage. Three in five businesses store data in the cloud, and 55 percent of businesses trust the person who built or administered their cloud environment did so securely.

"So many businesses have embraced cloud data storage, believing that placing their data in the cloud takes away all of their responsibility for security, when in reality this couldn't be further from the truth," notes Bailey.

"It is important businesses understand the joint role necessary to ensure data is secure. The cloud doesn't automatically mean your data is safe, and businesses still need their own data security policies in place. Never place all your trust in the cloud."

Taking cybercrime seriously

Bailey says he is encouraged that more businesses are taking cybercrime seriously.

“It used to be that cyber security was only a job for the IT department, not something for senior executives to put on the agenda. I’m pleased to see more than 90 percent of respondents say their Board or senior management is now engaged in cyber security, and two thirds say senior management see cyber security as a key concern or risk.”

The fact that 70 percent of respondents to Aura Information Security’s survey expect cyber-attacks to become more frequent and more sophisticated is a sign that organisations are beginning to understand the growing threat.

“Businesses recognise the dangers and now they must prepare for them. They should actively seek the weak points in their system with regular penetration testing so they can patch things up before hackers get a chance to attack.

“It’s also important to prepare for the worst. Assess the impact a data breach would have on the business and be sure to have a response plan in place, so you know what to do if your network is compromised,” says Bailey.

ENDS

© Scoop Media

Find more from Pead PR on InfoPages.

Business Headlines | Sci-Tech Headlines

BUSINESS, SCIENCE & TECH

Taskforce Report: Changes Recommended For Winter Grazing

A Taskforce has made 11 recommendations to improve animal welfare in intensive winter grazing farm systems, the Minister of Agriculture Damien O’Connor confirmed today. More>>

ALSO:

- NZ First - NZ First Welcomes Commitment to Improving Animal Welfare
- ***Image** via* RNZ - Winter cropping practices 'unacceptable' - govt

Consumer NZ Testing: Nine Sunscreen Brands Fail Protection Tests