• JANUARY ISSUE

TECH SECURITY INSIGHTS

Practical cybersecurity insights, advice and a true tall story every month

THE LATEST ON CYBERSECURITY:

1 How to protect your AI

2 Quick Tips

3 True Tall Story

Contact details for this month.

How to protect your AI

Your AI could be manipulated, poisoned, taught the wrong things or even stolen. How can you protect it?

AI has become an essential business tool. However, your AI needs protection from new, sophisticated threats designed to steal, exploit or corrupt your data.

New Threats in the AI Age

There are different ways your AI can be compromised. In this issue, we'll look at two of these and how you can protect your system from these attacks.

In both cases below, the attacker could use the information and access they've gained to ransom the company.

Even if the company pays the ransom, it would still need to rebuild its AI system and find a more robust way to protect AI system and find a more robust way to protect it.it.

QUICK TIPS

Your Human Firewall

Is your human firewall up-to-date?

As social engineering techniques become more sophisticated, it is vital to teach staff how to recognise and resist them.

Show them how scammers use their mind against them to try and trick them into giving them access to your systems.

Have a regular digital clean-up

Help keep your systems safe by archiving old data (away from your network), removing unused accounts and checking app and software permissions.

Remember to check on work-from-home accounts and devices that are taken off-site.

True Tall Story

In 2016, a group calling itself 'The Shadow Brokers' announced they'd hacked another group 'The Equation Group' and stolen their hacking tools.

The Shadow Brokers offered to auction what they'd stolen.

A case of hackers hacking hackers.

The Dangers of Data Poisoning and Integrity Attacks

AI-driven recommendations can help increase sales but can also be a significant risk to a business if they are not protected.

Data poisoning and integrity attacks are two ways hackers can disrupt your recommendation system. Bad actors know that if they can reduce the integrity of recommendations, they can damage the business.

Don runs an online retail business and has trained an AI to suggest other products based on information such as previous purchases and browsing behaviour.

To disrupt Don's business, the hacker creates a lot of fake customer accounts. The hacker then browses unrelated items and ones with high return rates; they buy them and then cancel the order to manipulate the AI's learning process.

What can Don do to protect his business?

Don uses an anomaly detection algorithm to identify and isolate any suspicious activity. This algorithm looks for anything unusual, such as increased cancelled orders.

Don's team reviews the data collection and processing stages when an unusual pattern appears. They can then identify and remove the corrupted data so the AI system works correctly.

Preventing Model Theft and Inversion Attacks

Model theft and inversion attacks can jeopardise data security and give hackers information they can use against the company.

Tina uses a custom-built AI model for risk assessment, forecasting, and scenarios for international clients. A hacker scans the company's network and finds a device with its default credentials in place; this is used as a 'backdoor' to steal the AI model.

Over several months, the hacker will use specially crafted queries to find sensitive client information without directly accessing the databases.

What can Tina do to protect her business?

Regular audits of the company's security, hardware and software will identify any devices that could be compromised.

Tina can also divide the network into smaller subnetworks to limit access to critical data. Each subnetwork has two-factor authentication, the latest encryption and security protocols. She also limits who has access to the subnetworks.

It may seem like hackers have an AI edge, but solid systems and forward-thinking can give your company an edge.

Are you concerned about how safe your AI is? Call us today and speak to one of our experts.