Why Automotive Dealerships Need to Beware in 2017

Why Automotive Dealerships Need to Beware in 2017

In 2017, experts predict an increase in professional, advanced attacks – including attacks on cloud infrastructure – and the rise of data manipulation attacks, further underlining the need for a fresh approach to cyber security.

Pentana Solutions and CyberHound have been working closely together for over 12-years to deliver high quality, reliable security solutions to customers. Cyber security threats are constantly evolving and can have significant impacts for automotive dealers if appropriate security solutions are not in place.

How CyberHound Can Help?

CyberHound is one of Australia's largest providers of cyber security solutions, helping Australian organisations and government agencies reduce cyber risks.

CyberHound's solution is used by hundreds of automotive dealerships across Australia to proactively protect their networks whilst empowering them with the tools to increase productivity in their workforce.

The CyberHound solution offers the following key benefits:

- Enhanced Malware/Ransomware protection across web and email
- Robust network security – via our **Managed** Next Gen Firewall, including granular visibility and control of all traffic
- Enhanced internet performance and reliability
- Increased staff efficiency and productivity
- Provision and security of internal and guest networks, including Botnet detection
- Vulnerability shielding, including real-time web content reputation protection

What's Next?

Pentana Solutions customers currently using the CyberHound solution can contact **Mark Di Muzio** on **1300 737 060** to coordinate a Health Check. Health Checks ensures the configuration is optimised and all of the latest capabilities are being utilised. It also provides valuable timesaving and productivity benefits and includes administration training.

Top 5 Cyber Security Threats

01

Cyber Crime

Encompasses any criminal act dealing with computers and networks as well as traditional crimes conducted through the internet.

RISKS:
Ransomware; viruses; spear phishing; cyberstalking; fake 'free WiFi'; identity theft; fraudulent fund transfers.

BIG THREAT TO LOOK OUT FOR:
Ransomware infiltrates and exploits company networks for the purpose of financial gain.

FACT:
The number of incidents, threat variety and damage to Australian businesses will grow in 2017 due to the high availability and ease of implementation for hackers.

02

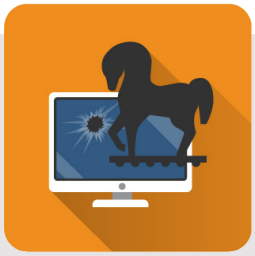
Cyber Attack

Deliberate attacks that try to manipulate, disrupt, deny, degrade or destroy computers or networks.

RISKS:
Distributed Denial of Service; botnets; website compromise; port scanning for backdoor access.

BIG THREAT TO LOOK OUT FOR:
Distributed Denial Of Service (known as DDoS) attacks involve flooding an organisation's internet and web services and significantly impairing networks.

FACT:
According to Deloitte, DDoS attacks for 2017 are expected to reach 10 million.



03

Social Media & Web Based Malware

Social engineering employs psychological manipulation and deceit to establish trust and elicit information.

RISKS:
Social engineering; malvertising (fake ads); watering holes; reputational threats; data leakage.

BIG THREAT TO LOOK OUT FOR:
Spear-Phishing refers to criminals who send emails purporting to be from reputable companies in order to induce individuals to reveal personal information.

FACT:
Symantec reported that targeted phishing attacks on businesses with fewer than 250 employees has and will continue to increase at an alarming rate.

04

Cloud Risks

As more businesses migrate their services to cloud managed solutions, vulnerability to hack attacks is more concentrated because of the concentration of computing resources and users in the cloud.

RISKS:
Compromised password security; data privacy and leakage; access from anywhere; ensuring reliable internet services and end point security are critical.

BIG THREAT TO LOOK OUT FOR:
Ensuring reliable internet access and password security / authentication for cloud apps and endpoint devices.

FACT:
Industry research shows that over 60 per cent of customers would stop using a company's products or services if a cyber attack resulted in a known security breach. This would have a catastrophic impact on any business, even if the breach was temporary.

05

The Insider Threat

An insider threat can be a malicious or just from careless behaviour from a member of staff. Careless behaviour includes posting confidential or inappropriate content on social media, losing an endpoint device or not using strong passwords.

RISKS:
Reputational damage, data leakage, intellectual property loss, financial penalties, loss of business revenue.

BIG THREAT TO LOOK OUT FOR:
Reputational damage and theft of trade secrets or customer information to be used for business advantage or to give to a competitive organisation.

FACT:
A Ponemon Institute/ IBM survey found the average cost of an Australian data breach was $2.82 million.