

Sundata briefing – IT security



LISTEN. RESPOND. DELIVER.



My background

- In IT since 1981
- 5 years at IBM
- 29 years in business
- Pearcey Award 2005 (Industry peer recognition)
- Founding member, & Chair Software Queensland
- Chair, ICT Industry Workgroup
- Fellow, Australian Computer Society

Sundata overview

- Established 1986
- 150 clients, mainly corporate
- Primarily engaged in IT infrastructure provision and support
- Services
 - Managed IT, Projects, Contract
- Privately owned
- Staffing @ approx. 45 full time equivalents
- Turnover this year @ \$15m AUD

How come Security is the number one IT issue in 2015?

A business level discussion about IT security

- The landscape
- The threats
- What can you do about it?
- Messages for your IT team or providers

What does an attack look like?

A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks.

Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

Consequences?

Cyberattacks may include the following consequences:

- Identity theft, fraud, extortion
- Malware, pharming, phishing, spamming, spoofing, spyware, Trojans and viruses
- Stolen hardware, such as laptops or mobile devices
- Denial-of-service and distributed denial-of-service attacks
- Breach of access
- Password sniffing
- System infiltration
- Website defacement
- Private and public Web browser exploits
- Instant messaging abuse
- Intellectual property (IP) theft or unauthorized access

What does this really mean?

- You (may) lose confidential data
- Your data may be corrupted
- You lose access to your systems
- Your clients lose access to your systems
- Your website is changed or access is denied
- Your systems are used for malicious purposes
- Your staff may be personally exposed
- Your clients may be exposed
- Emails go missing
- Your electronic reputation is compromised

The landscape – this weeks headlines

- Hackers demand huge ransom from banks to avoid DDoS attacks
- Hackers remotely turn off engine and jam brakes of car
- Ashley Madison hacked: Sensitive customer data from cheating website leaked online
- Cybercriminals go where the money is – SMEs
- Why small firms struggle with cyber security?

SME perspective

Keeping cyber thieves at bay is hard. They are busy, well-motivated and well-financed.

Daily, they produce about 250,000 novel variants of viruses.

Their vigour has helped them steal data from global companies.

Target, Home Depot and eBay, in the last few months.

This is even more acute for smaller firms.

We have an even tougher time keeping the bad guys out.

What to do?

Here are some examples of what not to do

- Give all your staff the same password when they join the company & then never change it
- Let your IT manager use bit torrent during the day, to download movies to his home PC
- Ensure your backups don't work by not changing tapes
- Switch off auto update of anti virus, because it's 'too much trouble'
- Publish the systems admin password to most staff (yellow stickys are good)
- Encourage your staff to share passwords to bypass problems
- Never test data recovery
- Go live with new systems without sufficient testing

Top 5 passwords of 2014

- 123456
- Password
- 12345
- 12345678
- Qwerty

So what can you do?

Education & compliance of Users

- Password robustness
- Phishing
- Malicious sites
- Malvertising

So what can you do?

Prevention

- Firewall hygiene (filtering traffic),
- Anti virus up to date
- Password robustness
- Physical security
- Encryption
- File management

So what can you do?

Mitigation

- Complete backups
- Tested for recovery
- DR or failover plan (tested)
- Mobile device management

Message for your IT staff or provider?

- Confirm they understand the seriousness of this threat
- Report on the state of play of the previous 3 slides
- Build a plan to achieve & maintain an agreed standard

More help?

Sundata can assist with building your IT resilience.

- Security
- Disaster Recovery
- Performance
- Reliability

Contact Kon Kakanis for more information.

kkakanis@sundata.com.au

0417 635265