Protection on a budget

Stuart Coulson
Business Liaison
Agenda

- Introduction
- What can you do about protecting yourself without it costing the earth
  - Tips one to five
  - Summary
- Final Thoughts
- Q&A session
Introduction

- Welcome!

- If you are tweeting during this presentation ... remember the tweet tags:
  - @UKFast
  - #CSC2011

- My esteemed colleagues – thank you!
If you are tweeting during this presentation … remember the tweet tags:

- @UKFast
- #CSC2011

The day after the presentation of the day before! – Reality Check!!
Introduction

- Question …

- What is your current planned budget spend on Cyber Security?

- What do you think your business thinks you should be spending on Cyber Security?

- Do you think it should be more than your current budget?
Your future is our business

The Big Question

Fully Comp
- IDS
- MX Filter
- DDoS Protection
- Firewall
- Pen Testing
- WAFs

3rd Party
- I’ll be OK
No magic ...

5 simple tips!
Tip 1

Passwords

Pa55w0rd
Passwords

5 Numbers long

- e.g. 12345
- It can be instantly cracked

5 characters mixed upper and lower case alphabet plus numbers and common symbols

- e.g. M@te5
- takes 13½ Mins to crack

SOURCE: http://www.lockdown.co.uk/?pg=combi
Hacker Tools

IHashGPU – by Ivan Golubev
This uses graphics cards to crack passwords.

- nVidia GTX 260 w/ 192 SP peaks at:
  - 560M/s MD5 hashes
  - 175M/s SHA1 hashes.

- ATI HD 5970 peaks at:
  - 5600M/s MD5 hashes
  - 2300M/s SHA1 hashes.

- http://passcracking.com/

£60
£400
FREE
“What’s worse is that every bit of data we took wasn’t encrypted.

Sony stored over 1,000,000 passwords of its customers in plaintext, which means it’s just a matter of taking it.

This is disgraceful and insecure: they were asking for it”

Big Questions

- How do I check if I have a vulnerability to see if my passwords are unencrypted and will end up being published on the internet?

- If I do have the vulnerability, what do I do about it?
Tip 2

Compliance
Buy Compliance

Get 2 vulnerability scans!!

Your future is our business
Tip 3

Knowledge
Knowledge is Power

1. Dr. Daniel Prince, ICT Focus
2. Stuart Coulson, UKFast
3. Richard Henson, The National Computing Centre
4. Tony Richardson, Octree
5. Tony Dyhouse, ICT KTN
6. Daniel Hunt, Get Safe Online
7. Prof Awais Rashid, Isis Forensics
8. Andrew Tyrer, Technology Strategy Board
9. Dave Lund, HW Communications
10. Dr. Bela Chatterjee
11. Dr. Mark Lacy
12. Dr. Daniel Prince
13. Dr. Paul Smith
14. Dr. Coral J. Dando
Tip 4

Cost Versus Risk
Your future is our business

Tolerance

Likelihood

Impact on my business

Low

High

I accept this risk

Uh Oh !!
An Example

**Scenario**
I am an online candle sales shop.

**CONFIDENTIALITY**
visitors details (including credit cards)

**INTEGRITY**
what if someone changes the site?

**AVAILABILITY**
this is my only source of income

Your future is our business
Tip 5

Have a plan

Know what do you do if you’re hit
1. Freeze
2. Notify
3. Rebuild

Your future is our business
A client of UKFast was attacked by a leaky SQL database.

We know the attacker was tn_scorpion (they left a nice calling card to say so)

They also gave an email address to their group to contact them.
Say hello ! To Raouf Besrour

Information identified
Twitter
Facebook
Myspace
Legacy Personal Site
LinkedIn
Mobile Number
Address
Photograph

Your future is our business
Summary

(I’m nearly done!)
Summary of the Tips

1. **Passwords**
   - Long and complex
   - Encrypt your password databases

2. **Compliance**
   - ISO9001, ISO27001, PCI DSS

3. **Knowledge**
   - Use experts

4. **Cost Versus Risk**
   - Know your risks

5. **Have a plan**
Final Thoughts

And thank you!
Final Thoughts

But a lot of businesses out there don't see the return on investment, they look at it as a liability, and until they can understand that proactive security actually gives them a return on investment, it's still a hard sell for people.

Kevin Mitnick
Knowledge is free
We are anonymous
We are legion
We do not forgive
We do not forget
Thank You for listening

Expect us

Anonymous (2011)

Your future is our business