Security, Your Business

SOME STUFF YOU SHOULD KNOW, SOME STUFF YOU CAN DO
Myself

PhD Student at UMD
  ◦ Programming Languages and Security

Systems Engineer at Trail of Bits
  ◦ R&D on applied research in application security

Previously Kyrus
  ◦ Carbon Black, kernel level system integrity monitoring
    ◦ Since acquired by Bit9, congrats!
  ◦ Collaboration with Microsoft on Zeus botnet takedown
The Threat Portrayed

Security consultants say don’t get hacked, your business...

◦ Will fail
◦ Customers will leave
◦ New customers won’t show up
◦ Your stock price will tank
◦ You’ll get sued
◦ Regulators will penalize you
Some Big Examples

Heartland payment processing
- Infiltrated payment exchange system
- Massive dumps of valid CC data directly from the backend

HBGary e-mail leak
- Full, indexed dump of all e-mail the company sent or received in its lifetime

Perhaps this produces a few rules
- Do not antagonize Anonymous
- If you do, have a contingency plan more substantial than “go on to IRC and plead with the people who hack us”
Some Big Examples

LastPass
- Assumed full dump of LastPass online database

Comodo
- Hacker gained ability to sign certificates of their choice with Comodo key

5. Here is another proof:
7. I uploaded JUST 1 table of their ENTIRE database which I own.
8. Also ask Comodo about my hack, ask them what I did to them. Let me tell you what I did:
Some Of These Are Pretty Bad

Comodo is a PKI Certificate Authority
They sign CSRs for money
Their business is supposed to be choosing the right CSRs to sign
Their business is literally providing trust
They failed
They’re not alone, other CAs have fallen in similar ways
People still use them though…
The Threat Deflated

How many companies have gone under because they were owned?
  ◦ Maybe two
    ◦ And one of them is mtgox

Every company previously is still around
  ◦ HBGary was sold
  ◦ People I know still use LastPass
  ◦ Everyone still uses Heartland payment processing on the backend

If getting hacked is so bad, then why are they still around?
Unwarranted Cynicism

Maybe all the security people are full of crap

Maybe all the security people just want job security
  ◦ There’s probably some truth in this
  ◦ A lot of the security industry definitely does not want to see security actually “solved”

Customers see getting hacked as a natural disaster
  ◦ You wouldn’t blame a business when their office is hit by a tornado

We do have some useful things to tell you though
## What Threats Do You Face?

So given this, what kind of threats will your new businesses face?

<table>
<thead>
<tr>
<th>Threat</th>
<th>Opportunistic</th>
<th>Targeted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disruption</td>
<td>DDOS for Money</td>
<td>DDOS for a cause</td>
</tr>
<tr>
<td>Intrusion</td>
<td>Drive-By, Cryptolocker</td>
<td>Very motivated criminal enterprise</td>
</tr>
</tbody>
</table>

---

**Tech Start-Ups Are Targets of Ransom Cyberattacks**

By NICOLE PERLROTH and JENNA WORTHAM  APRIL 3, 2014, 4:00 PM  8 Comments
What Can You Do?

Don’t panic about security
◦ Being told “you’re going to lose” shouldn’t be scary – it should be freeing

Think early about how to respond to security reports
◦ Having a security@ for your company is a good step
◦ Not freaking out and trying to downplay the issue is also good

Please don’t use C
◦ C is like leeches, we used it before we knew better, but now we have science and technology

Don’t antagonize angry teenagers on the Internet

Google “matasano chargen indie security” and read the first hit
◦ Do it now
Indie Security 12(ish)-step

<table>
<thead>
<tr>
<th>Prioritize security with your other goals</th>
<th>What else will kill the business first?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do outreach correctly</td>
<td>Have a security page, don’t argue with the security community</td>
</tr>
<tr>
<td>Practice basic code hygiene</td>
<td>Zero-init, abort on malloc failure, whitelist content to alpha-numeric</td>
</tr>
<tr>
<td>Just don’t do some things yourself</td>
<td>Cryptography, passwords, installers, file download/upload</td>
</tr>
<tr>
<td>Deploy Rubber Chicken Security</td>
<td>Get PCI certified, use SSL</td>
</tr>
<tr>
<td>Fuzz test your app</td>
<td>Buy and learn burp</td>
</tr>
<tr>
<td>Don’t treat code as secret</td>
<td>Assume all your code will be known</td>
</tr>
</tbody>
</table>
Security Is Largely An Ethical Concern

The market won’t reward you for having good security

So your motivation for doing security well will be internally motivated

Your concerns should be proportional to the severity of information that you are trusted with
  ◦ Facebook for dogs? Ehh...
  ◦ A communication system for activists in hostile countries? Hmm...

Your customers will stick with you through good and bad security
  ◦ Your memories of the problems your customers have due to your bad programming will be with you for life though
  ◦ Learn things about security or get a good Scotch habit
Growing up

Maybe you never need to really care about security

Maybe one day, you’ll have a lot of things that other people want
  ◦ Lots of data about people in the world
  ◦ And their money
  ◦ A large install base of very vulnerable code

When that day comes, you should probably grow up
  ◦ Give us a call ;)}
In Summary

You will have to care about security, nobody else will
A lot will motivate you not to care
There are some focused things you can do to improve your security maturity without compromising your business agility
Things are pretty bad, but not as intractable as they might seem

https://github.com/isislab/Hack-Night
andrew@trailofbits.com