DATA SECURITY CHALLENGES IN THE ALL TOO PUBLIC AND NOT SO PRIVATE SECTORS

Patrick Gray
Principal Security Strategist

CISCO

FIRST
I want you to take home four points

- Understand
- Educate
- Collaborate
- Prepare
It’s a great to be in Vienna today, but uh, do you know where your data is right now?
It’s all about data, your data

- The confidentiality
- The integrity
- The availability
It’s hard to protect that which we have no idea as to its whereabouts

- So, where is your data today?
- It’s in the cloud
- On any device
- Any place
- Any time
When “aren’t” we working anymore?
Mobile Apps
Your apps
Today, it’s about mobility...

- In the past few years we shifted our lives to the PC and the Internet
- Now, it’s all about being mobile
- A PC in your pocket
- Our mobile work force is growing and expanding
Where?

- Where does work happen?
It happens wherever we are!

- No longer does business take place solely behind network walls
- The critical work is happening increasingly on social networks, on handheld devices, in the field, and at local cafes
The traditional perimeter, with clearly identifiable boundaries, has diminished

In its place, a network with limitless potential is rising

One where Universities, agencies, companies, their customers, and their partners demand access to information whenever and wherever they need it
New Considerations

- It is information technology’s role to ensure that the appropriate people, using the correct devices, are accessing the proper resources while having a highly secure yet positive user experience within your networks.
A blurring of activities

- In addition, it is common for workers to blend business and personal communications on these social networks, further blurring the network perimeter
Where are we going and what are we doing?
Some bone-jarring statistics

- 50% of Facebook active users log on to Facebook on any given day
- More than 60 million users update their status daily
- People spend over 500 billion minutes per month on Facebook
Billions

- More than 3 billion photos uploaded to the site each month
- More than 5 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each week
The involvement is viral

- Millions of local businesses have active Pages on Facebook
- More than 20 million people become fans of Pages each day
- Pages have created more than 5.3 billion fans
Mobility

- There are more than 200 million active users currently accessing Facebook through their mobile devices
I just have to check...

- Checking your Facebook account has become the default Water Cooler
- It's the most commonly visited website at the workplace, twice as popular as Google and three times as popular as Yahoo
The keypad is mightier than the sword
If you think it’s a fad, think again...
Cisco on Facebook
Cisco on Twitter

Understanding the Trust Gap: Certificate-Signed Malware (new Cisco Security blog post)
http://j.mp/cYgfJ7
32 minutes ago via FurlTwitter V2

@windemier Being awesome in IPS? I'm missing the humor
Unless you're talking abt the electrical female/male parts story.
That was amusing.
about 2 hours ago via web in reply to windemier

@GeekChickUK Yes?)
about 2 hours ago via web in reply to GeekChickUK

Wooh! RT @infosecurity: Cisco's top-dog status confirmed in new IPS vendor ratings survey: http://j.mp/Z9gQX @SecurityJeff
about 2 hours ago via web

@standaloneSA I used to hear that in lab. The other students were actually talking abt electrical components but it still weirded me out.
about 2 hours ago via web in reply to standaloneSA

Cisco's Security Week in Highlights: Cyber Risk Report
http://j.mp/8O6Ey
about 3 hours ago via FutureTweets V2

Cisco on YouTube
FIRST
Vienna on Facebook
Graz

Graz, Austria
City

Description
From Wikipedia, the free encyclopedia

Graz is the second largest city in Austria after Vienna and the capital of the federal state of Styria. On 1 April 2010 it had a population of 261,860 (of which 268,678 had principal residence status).

Graz has a long tradition as a student city; its six universities have more than 44,000 students. Its "Old Town" is one of the best-preserved city centres in Central Europe.

Politically and culturally, Graz was for centuries more important for Slovenes than Ljubljana, the capital of Slovenia, and still remains influential.

In 1999, Graz was added to the UNESCO list of World Cultural Heritage Sites, and the site was extended in 2009 by Schloss Eggenberg. Graz was the Cultural Capital of Europe for 2003 and got the title of a City of Culinary Delights in 2008.

Geography

Graz is situated on the Mur River in the southeast of Austria. It is about 200 km (120 miles) southwest of Vienna. The nearest larger urban center is Maribor in Slovenia which is about 50 km (31 miles) away. Graz is the capital and largest city in Styria, a green and heavily forested area.

Nearby Places

- Stadtspark Graz
  298 check-ins - 204 likes

- SCS
  577 check-ins - 253 likes

- Uni Resowi
  357 check-ins - 57 likes

People You May Know

Jocelyn Gray
has poked you.

Ron Dilley
Instant friend
Add as friend

Sponsored
Go Tankless, Save $800
chooseaeroplumbing.com

Save money and energy with a tankless water heater from Aerow. Plumbing Call today to save ups to $800 through rebates & tax credits!

Natural Release Massage

30 minutes FREE for your first session at the Revival location. SAVE $50, 90 minutes for $85, 2 hours for $100.

Like this - 60 people like this
This is viral

- Overall, Facebook is now used by 1 in every 13 people on earth
What else are they doing?

- Over 250 million people interact with Facebook from outside the official website on a monthly basis, across 2 million websites.
Austrian Facebook users

There are over 2,559,180 Facebook users in Austria
There is a human element to all of this, an element that is more often than not, overlooked...
It’s no longer just close relationships

- Our employees are going places they’ve never gone before and are touching technology daily
- That which they are touching is touching our networks as well
That being said...

- There are things we really need to be aware of.
- The bad guys know what we’re doing, where we’re going and want to make the trip a wee bit more difficult.
With Web 2.0

- A new breed of malware is evolving
- Google Mashups, RSS feeds, search, all of these can be misused by hackers to distribute malware, attack Web surfers and communicate with botnets
Risk – it's everywhere

- And no one knows that better than IT security professionals
- Disgruntled employees, students, fired employees, clueless employees who succumb to social engineering, passwords left on Post-it notes, wide-open instant messaging and increasingly powerful hacker tools in the hands of teenagers, Web Mobs and Organized Crime targeting Social Media sites
Objective?

- The key objective, of course, is to recognize risk, safeguard your reputation and not reveal sensitive or confidential information that may prove quite harmful.
Two biggest vectors for Malware

- Email
- Web-based
The Human Firewall – an invaluable tool

- A good *human firewall employee* is one who filters good security practices and rejects any others—much like a network firewall only allows authorized traffic and rejects any other

- The only way to build a good human firewall is to raise people’s awareness; to teach them good habits, to make them recognize bad practices and change them into good practices

- Your cyber security is only as good as the people who manage it and those who use it
So Patrick, why do we really need that Human Firewall?
Because, ‘Friend’ has become a verb

- Social media users believe there is protection in being part of a community of people they know
- Criminals are happy to prove this notion wrong
My new friends...

December 7, 2009 7:20 AM PST

Study: Facebook users willingly give out data
by Don Reisinger

263 reacted | Share | 179

Facebook users are too willing to give out their personal information, security firm Sophos has found.

According to Sophos' Australian team, which conducted a study to see how likely Facebook users were to offer up personal information, 41 to 43 percent of the 100 people Sophos contacted "blindly accepted" friend requests from two fake Facebook users created by the security firm.

After becoming friends with Sophos, the security firm was able to access up to 89 percent of the users' full dates of birth, all of their e-mail addresses, where they went to school, and more. Half of all the users Sophos befriended displayed the town or suburb where they live. They even offered up information on family and friends.

Younger users were "more liberal" with their workplace or school information than older users. "Both groups were very liberal with their email addresses and with their birth dates," the security firm wrote in a blog post Sunday, announcing the results. "This is worrying because these details make an excellent starting point for scammers and social engineers."

The security firm added that "10 years ago, getting access to this sort of detail would probably have taken a con artist an identity theft several weeks, and have required the on-the-spot services of a private investigator. Sad to say, these days, many social networkers are handing over their life story on a plate."
Causation

- The threats and security issues that come with social media aren’t usually caused by vulnerabilities in software.
- More commonly, these threats originate from individuals who place an unwarranted amount of “transitive trust” in the safety of these communities.
Remember...

- On social sites –
  - Your privacy is history
  - They don't have your best interests in mind
  - Social engineering attacks are getting more targeted
Trust?

- Users will trust something or someone because a user they know has also expressed trust in that person or subject
- We trust because we are curious and curiosity...
Curious? This is why! Out of date???
They want to send us somewhere else...

From: Automated Clearing House (ACH) [mailto:***@nacha.org]
To: ***@***.com
Subject: Unauthorized ACH Transaction Report

Dear bank account holder,

The ACH transaction, recently initiated from your bank account (by you or any third party), was rejected by the Electronic Payments Association. Please review the transaction report by clicking the link below:

Unauthorized ACH Transaction Report

Copyright ©2009 by NACHA - The Electronic Payments Association
The unknown... DO NOT TOUCH THIS!!!

XP antivirus Online Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is strongly recommended to remove them immediately.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Risk level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware.IEMonster.b</td>
<td>Spyware</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>Zlob.PornAdvertiser.Xplisit</td>
<td>Spyware</td>
<td>High</td>
</tr>
<tr>
<td>Trojan.InfoStealer.Banker.s</td>
<td>Trojan</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Remove All   Ignore
To help protect your computer, Windows Firewall has detected activity of harmful software.

Do you want to block this software from sending data over the Internet?

Name: Trojan-Spy.Win32.GreenScreen
Risk Level: CRITICAL
Description: This is spy trojan that installs itself to the system, hides itself and then captures screen images and saves them to disk files in encrypted form. Thus it allows to a hacker to watch screen images.

Keep Blocking  Unblock  Enable Protection

Windows Firewall has detected unauthorized activity, but unfortunately it cannot help you to remove viruses, keyloggers and other spyware threats that steal your personal information from your computer, including your Credit Card data and access passwords to the online resources you use. Click here to pick recommended software to resolve this issue.
YOUR SYSTEM MAY BE INFECTED!

Scanning:

Internet threats and viruses found:

FREE SCAN NOW!
This is what our users are up against...
Malware popping up out of nowhere!

- Don’t go there!
- Stay on the path that you know well!
- Okay to trust but please verify
- So, have fun! But monitor...
- Be a bit more vigilant
- And manage appropriately
But what does all this mean?

- I am just a user and am not an engineer or a technician or a programmer or a geek!
- I’m just sitting at my desk, talking to friends and all sorts of people
- How in the world am I threatening our network???
2 Reasons...

- You probably do not understand policies, procedures, best practices and standards
- If you do understand them, they are violated because there are no consequences – the policies are not enforced
- Who, me?
The Seven Deadly Sins of Network Security

1. Not measuring risk
2. Thinking compliance equals security
3. Overlooking the people
4. Lax patching procedures
5. Lax logging, monitoring
6. Spurning the K.I.S.S.
7. Too much access for too many
The Opposing Team

- The Hackers
- Disgruntled Insiders
- Clueless employees
- Competitors
- Foreign Governments
- Terror organizations
Top 8 Perceived Threats

- System penetration
- Sabotage of data
- Theft of proprietary information
- Denial of service
- Viruses and Worms
- Unauthorized insider access
- Laptop theft
- Insider abuse of the Internet
System Penetration

- It is an unfortunate reality that you will suffer a breach of security at some point
- To bypass security, an attacker only has to find one vulnerable system within the entire network
- But to guarantee security, you have to make sure that 100 percent of your systems are invulnerable -- 100 percent of the time
Not good...

- But Patrick! It won’t happen to us!
Whether you get hacked depends...

- Do you assume the posture of, “It can’t happen here.”
- Do you hear, “We haven’t heard of any worm outbreaks and all seems quiet. Why upgrade those devices?”
- “We have no budget.”
- “We’re just hanging out in Vienna!”
- “They’re only going after the Government and those really big banks.”
- Then my question is, “Can you really afford to give up data today?”
You can’t afford to give up data, so be prepared and alert...

- “Every man has a plan, until he gets hit!”
- Watch for anomalous behavior
So, what are they really after?

- Your data
- Your assets
- Your employee’s data
- Your personal data
- Your paycheck
- Your friends
- Your family
Know who to call...
You are the last line of Defense! Step up!

- Understand
- Educate
- Collaborate
- Prepare
Thank You!

pagray@cisco.com