The risks and rewards of Social Media and Enterprise 2.0
(and why your role is so important)

John Rezabek  CISSP
jrezabek@paloaltonetworks.com
enterprise 2.0 applications take many forms

Enterprise 2.0 has arrived
user expectations of enterprise 2.0 applications

Base: 303 social media and online users in full-time employment

Source: January 2010 Social Media Users Online Survey
five things to know about enterprise 2.0

1. Driven by new generation of addicted Internet users – smarter than you?
2. Full, unrestricted access to everything on the Internet is a right
3. They’re creating a giant social system - collaboration, group knowledge
4. Not waiting around for IT support or endorsement – IT is irrelevant
5. Result - a Social Enterprise full of potential risks … and rewards
how will you respond to this challenge?

• How can I regain control of enterprise 2.0?

• What value do these applications provide to my business?

• What is my organization’s risk tolerance for these applications?

• How can I “safely enable” the right applications?

• Where do I start?
start by understanding what’s really happening

• Application Usage and Risk Report
  • Findings
    • 720 large enterprises worldwide
    • 900+ different applications
    • Employees have created Enterprise 2.0
  • Rewards
    • Enterprises are embracing social networking apps
    • Proven to deliver measurable value to business
  • Risks
    • Incoming threats are increasing
    • Potential for data leakage is increasing
    • Existing security infrastructure ineffective
what are the risks and rewards of these apps?
sharepoint reward - coca-cola

• Coca-Cola Enterprises
  • Centralized platform to promote initiatives to highly distributed workforce
  • 72,000 people in 431 facilities around the globe
  • 30,000 SharePoint users

• Benefits
  • Productivity and customer focus
  • Companywide intranet
  • IT transformation
  • Effective remote teams
  • Deskless worker access
sharepoint rewards – other success stories

- Connect users across 47 countries
- Immediate savings of $250,000
- 33% improvement in process for enhancing of 3,400 products
- Faster time-to-market through enhanced communications
- Connect users across 47 countries
- Immediate savings of $250,000
In total, more than 220,000 SharePoint threat instances were found. More than 30% of SharePoint deployments are “rogue”
another reason sharepoint is hard to control

Most Frequently Detected "Dynamic" Applications

- Sharepoint: 83%
- iTunes: 78%
- MS RPC: 77%
- Skype: 73%
- BitTorrent: 60%
- MSN Voice: 60%
- Ooyla: 55%
- Mediafire: 54%
- eMule: 51%
- Teamviewer: 42%
what should you do with SharePoint?

Balance risks and rewards

Block SharePoint?
Allow SharePoint?
Other option?
facebook – a useful enterprise 2.0 application

- The most popular communications tool on planet Earth
- 600 million + users and growing rapidly
- Average user has 130 friends
- People spend over 500 billion minutes per month on Facebook
- More than 70 translations available on the site

- Risk - More than 550,000 active applications on Facebook
- Reward - More than 250,000 websites have integrated with Facebook
Social Networking: Facebook Dominates

- Facebook was found in 96% of enterprises
- Facebook consumes 80% of the total social networking bandwidth;
- “Passive” aspects of Facebook make up over 92% of Facebook traffic
- “Active” aspects are minimal
facebook rewards – marketing and support

Invests 25% of marketing spend on social networking apps

On-line support “community” reduced support costs - $.25 vs. $12 per interaction

Launched GTI exclusively through and other social networking applications
facebook reward – virgin atlantic
facebook – risks to consider

- Facebook-specific worms (Koobface)
  - Delivers messages to 'friends' of a Facebook user whose computer has been infected
  - Prompts user to download Adobe Flash update; installs trojan virus instead
- Obfuscated/shortened links
  - Click here to download malware, not watch BBC video
- Data leakage
  - Users often say too much and post too much
- Facebook applications
  - Install an application = install a threat
facebook risk – 500,000 3rd party apps

New threat: Undetectable Facebook scams

Security smarts may not be enough to identify rogue Facebook apps. But a little patience may help.

Erik Larkin (PC World [US online]) 29/04/2010 08:32:00

Tags: security, Facebook

I recently received two Facebook e-mail notifications that set my security spider-sense tingling. Nothing was obviously wrong with the e-mail messages, which said that my friend had tagged a photo of me and then commented on it. But something about a reference to an app named "Who stalks into your profile" just didn't feel right.

So I checked it out. I dug into the e-mail header to make sure that it was from Facebook—it was. A search for the app's name didn't turn up any warnings. The app's installation page didn't give me any obvious clues, either. Still, I let my paranoia have its day, and I sat on the app.

Sure enough, it was a scam, and an ingenious one. When anyone installed the supposed stalker app, it first created a photo montage of friends' images and then commented on that montage. Facebook duly sent out "your friend tagged a photo of you" messages, effectively advertising the scam app, which was created to generate illicit online ad revenue.
what should you do with facebook?

Balance risk and rewards

Block Facebook?
Allow Facebook?
Other option?
What about the risks and rewards of these applications?
should all employees be allowed to tweet?
what files are employees sharing?
is it ok to bypass security controls?

UltraSurf
Privacy, Security and Freedom

UltraSurf 9.95
Free Download

Privacy
Protect Internet privacy with anonymous surfing and browsing -- hide IP addresses and locations, clean browsing history, cookies & more ...

Security
Completely transparent data transfer and high level encryption of the content allow you to surf the web with high security.

Freedom
UltraSurf allows you to overcome the censorship and blockage on the Internet. You can browse any website freely, so as to obtain true information from the free world.

Facts of UltraSurf:
- Service provided for 7 years
- Millions of users
- Users from over 180 countries
- Daily hits over 800 million
- Daily traffic over 8,000 GB
Applications Are The Threat Vector

US$3.8M stolen from small school district in New York State

- Zeus banking trojan stole credentials, enabled transfers
- All but US$500K recovered

Increasingly, new and old threats using social networks

- Social network-specific (e.g., Koobface, FBAction)
- New life for old threats (e.g., Zeus/Zbot)

Huge user populations, high degree of trust, liberal use of SSL
Social Networking: Strengths

- Reaching new people, deepening existing relationships
- Reduction in cost of sales/marketing (disintermediation)
- Reduction in cost of support
- Reduced time to collaborate
Social Networking: Weaknesses

• Virtually Unmanaged Today
  • Few policies
  • Existing policies aren’t enforceable
  • Savvy users
• Security models too restrictive
  • Coarse allow/deny
Social Networking: Opportunities

Evolve security policies
Evolve controls
Make risk management/security relevant
Top 10 Social Networking Threats

- Social networking worms
- Phishing bait
- Trojan vector
- Data leaks
- Shortened/obfuscated links
- Botnet command and control
- It’s a data source
- Cross-Site Request Forgery (CSRF)
- Impersonation
- Trust
Social Networking is A Hotbed of Risk

- **Data Loss/Leakage**
  - Unauthorized employee file transfer, data sharing

- **Network Intrusion**
  - New avenue for threats to enter the organization

- **Image Damage**
  - Mis-treat your customers/constituents at your own peril

- **Compliance**
  - Using unapproved applications, unaudited

- **Operations Costs**
  - Excessive bandwidth consumption, desktop cleanup

- **Productivity**
  - Uncontrolled, excessive use for non-work/mission related purposes
the underlying cause of the security problem

• Firewalls should see and control applications, users, and threats . . .

. . . but they only show you ports, protocols, and IP addresses – all meaningless!
What You See...with Port-Based FW + Application Control Add-on
What You See with a True Next-Generation Firewall
Existing Infrastructure Hasn’t Kept Up

Applications have changed
Any port or random ports
Evasive
SSL encrypted
Tunneled within other apps or protocols

• Users feel entitled to use any application
• New employees = always on, always connected
adding more stuff doesn’t solve the problem

- Complexity and cost increase
- Performance decreases
- Still no visibility or control of enterprise 2.0
Some attempts with Slow Multi-Pass Architecture – UTM?

- Based upon arcane technology
- Still Can’t Control Applications
- Can’t scale for multigig networks
- Increased complexity works against principals of security
intelligence and control belongs in the firewall

- The firewall is the right place to address the emerging security challenges
  - It sees all traffic
  - It defines the trust boundaries of the network
  - It is the device that most tightly integrates with security operations
  - It is the most pervasive product deployed
**time to transition to next generation firewalls**

1. Identify applications regardless of port, protocol, evasive tactic or SSL
2. Identify users regardless of IP address
3. Identify and prevent potential threats associated with all high risk applications
4. Granular policy-based control over applications, users, functionality
5. Multi-gigabit, in-line deployment with no performance degradation
solutions from industry’s “most visionary” vendor

Firewall + IPS + URL + AV + Policy + Reporting + Performance

Exceeds requirements for NGFW defined by Gartner
innovations that transform the firewall

**App-ID**
Identify 1,200+ applications

**User-ID**
Identify every user – by name

**Content-ID**
Scan and control all content
hardware architecture optimized for performance
total visibility into applications, users, content

Filter on Skype and user Harris

What else is Harris using
Your Control With a Next-Generation Firewall

» The ever-expanding universe of applications, services and threats

» Traffic limited to approved business use cases based on App and User

» Attack surface reduced by orders of magnitude

» Complete threat library with no blind spots
  ✓ Bi-directional inspection
  ✓ Scans inside of SSL
  ✓ Scans inside compressed files
  ✓ Scans inside proxies and tunnels

» Only allow the apps you need

Safely enable the applications relevant to your business
unprecedented level of enterprise 2.0 control

- Now you can minimize risks, maximize rewards
  - Block bad apps to reduce attack surface
  - Allow all application functions
  - Allow, but only certain functions
  - Allow, but scan to remove threats
  - Allow, but only for certain users
  - Allow, but only for certain time periods
  - Decrypt where appropriate
  - Shape (QoS) to optimize use of bandwidth
  - …and various combinations of the above
fewer policies, but greater control

- Very simple, yet very powerful, control of applications, users, and content
learn more about more than 1,300 applications
now you can respond to this challenge!

• How can I regain control of enterprise 2.0?

  • What value do these applications provide to my business?

    • What is my organization’s risk tolerance for these applications?

  • How can I “safely enable” the right applications?

    • Where do I start?
what does your enterprise 2.0 look like?

• Request a free Application Visibility and Risk report

• Take back control of your network

• Make Enterprise 2.0 work for your business
Recommendations

• **Policy**
  - Gather
  - Listen
  - Redefine

• **Model – re-think or refine**
  - Blindly blocking is somewhat draconian; blindly allowing is a CLM
  - Safe enablement is your new mantra

• **Controls**
  - Visibility and control of applications, users, and content is key
  - “Allow, but…” controls are critical
Conclusions

- Social networking and social media applications are here to stay
  - High use, High risk, high reward
  - Applications and users are adept at circumventing controls
  - Changes in network security required – can’t blindly allow, can’t blindly block. Need safe enablement

- Can’t Do Security 1.0 in Enterprise 2.0 World
  - Existing controls inadequate
  - Adding more appliances isn’t the answer

- Next-Generation Firewalls Can Help
  - Identify and control applications, users, content
  - Safe enablement: no more flashlights and whack-a-mole
About Palo Alto Networks

- Palo Alto Networks is the **Network Security Company**
- Founded in 2005 by security visionary Nir Zuk
- Next-generation firewalls that identify / control 1,300+ applications
- Innovations: App-ID™, User-ID™, Content-ID™
- 4,500+ customers in 60+ countries, 24/7 support
- “Most Visionary” in Gartner 2010 Enterprise Firewall MQ
- Fastest growing firewall vendor in the world
thank you!