Data Security Threats: Education systems in the crosshairs

July 11, 2012
STATS-DC

Mike Tassey
Security Advisor
PTAC
Overview

- What does “threat” mean
- Who is behind all of this
- What do they want with my systems
- How can my systems be exploited
- What can we do to reduce the risk
What Does "Threat" Mean

- Threat has many definitions
- The singular truth is that “threat” requires vulnerability
- Understanding our vulnerabilities and the ways they can be exploited is the best insurance against the threat
Should We Worry?

- Data breaches, hacks, and privacy spills abound
  - Citigroup, VA, Sony, TJX, RSA, UNCC, Clarksville-Montgomery County School System...

- We face a lot of challenges
  - Applications security
  - Configuration management
  - Risk assessment

- It’s all about “risk,” knowing what your tolerance is
- Checkboxes don’t make you secure
- It’s easy to get lost between policy and execution
Who Are the "Bad Guys"

- Public Enemy #1.... It's "us"
Who Are the "Bad Guys"

- **Internal threats**
  - Misconfiguration, complacency, lack of awareness
  - Insiders (curious, careless, or disgruntled employees)

- **Criminal Threats**
  - Fraudsters, identity thieves
  - Organized cyber-crime
  - Identity black market

- **Hacktivist Threats**
  - Cyber-activists who attack for political, egotistical, or philosophical reasons
  - Anonymous, LulzSec
It's Getting Easier for Attackers

- Open source and free tools make it easier
- Free hacker training sites / forums
- Cyber-theft is commoditized
  - Black market for privacy data
  - Underground economy where tools are built and sold to order
  - 2 million new pieces of malware a year
- We are still developing flawed code
  - SQLi discovered in 1998, still in the OWASP Top 10
  - Cross-Site Scripting (XSS)
  - Session Management
  - Patching (especially 3rd party software)
Industry Effort vs. Attacker Effort

- Average 1-5 bugs for every 1,000 lines of code
- Even our security software is not immune
- Attack surface is getting bigger… not smaller
- It’s not “if” an attack will happen, more like “when”
- Have a plan

Source – Pieter “Mudge” Zatko (Black Hat 2011 keynote address)
What Do They Want?

- Identity information
  - Social Security numbers, addresses, birth dates, etc.
  - PII is used to obtain credit, purchase items, perform criminal activity
  - Thieves value children’s identities, because they are “fresh”
  - Some 10% of children may already be victims

- Disruption and damage
  - Denial of Service (DoS and DDoS)
  - Defacement of web sites
The Results...

I have uk cc, aus cc and us card for sale with alots of good bin / post code Contact me if you want to buy: Uk random cc Uk random cc with dob Uk cc with post code CC uk with bin CC uk with bin+dob CC uk with bin+bank acc+sortcode+dob Now i have alot of hot bin like 552213,530127,492940,492942... I never resell cc , all dead cc will be replaced instantly I accepct : LR and WU as payment method Contact me via Yahoo mail

=========> Here is the complete list of tools I'm sale and it's price.

========LIST AND PRICE CC + CVV FOR SALE =========

* Format is always: full info

| CARD TYPE | FIRST NAME | LAST NAME | CC NUMBER | EXPIRY DATE | CVV | ADDRESS | ZIP CODE | CITY/TOWN | STATE | COUNTRY | PHONE | DOB | SSN | MOTHER'S MAIDEN NAME | VERIFIED BY VISA | CVV2 | EMPLOYMENT | POSITION HELD |

List cc I have and price I have :
US (Visa, master) = $3 per 1 | (bin) = $10 | (dob) = $15 | (fullz) = $25
- US (Amex,Dis) = $5 per 1
- UK (Visa,Master) = $8 per 1 | (bin) = $15 | (dob) = $20 | (fullz) = $30
- UK (Amex,Dis) = $13 per 1
Why Me?

- Education systems are increasing in size and complexity, warehousing lots of PII
- Search engines make targets easier to find
  - Robust search engine functionality can help attackers pinpoint vulnerable systems
  - Good guys use Google too
- Mobile Users / Mobile Workforce
  - Administrators and users take their work on the go
  - Use untrusted networks
  - Lost / stolen devices or media
How Do They Do It?

- Internet-facing Applications
  - OS remote vulnerabilities are on the decrease, attackers are focusing on your applications
  - Developers still lagging in implementing secure coding practices

- Client-side Attacks
  - Phishing, click-jacking, browser exploits, plug-ins
  - Malware (spyware, adware, trojans, rootkits)
  - Mobile users (wireless, hostile networks)

- Physical threats
  - Shoulder surfing, dumpster diving, evil hardware
  - Lost or stolen hardware
How Can We Stop Them

- Nothing is 100% secure
- Create a Culture of Awareness
  - Awareness training programs
  - Leadership needs to be on board, leading the charge
- Know your systems and their vulnerabilities
  - Identify the “Crown Jewels” and protect them first
  - Ongoing assessment of security posture and risk
- View your own systems like you mean to do harm
- Standardize (technology, data, procedures)
  - Adopt common methodologies
  - Band together with partners & share threat data
How Can We Stop Them

- Mitigate the threat
  - People are the key, awareness is a powerful weapon
  - Make what you already have work better
  - Leverage technology, but don’t rely on it

- Monitor & manage your data
  - Use tools to make monitoring easier
  - Collect logs that make sense

- Be ready to respond
  - Have a response plan
  - Identify the response team in advance and set aside the resources needed
  - Periodically test response capability with simulated events
PTAC Resources

- Currently Available
  - Data Security Checklist
  - Data Governance Checklist
  - Cloud Computing FAQs
  - Authentication Best Practices
  - Data Breach Response Checklist
PTAC Assistance – Site Visits

- PTAC can come to your location and provide review and advisory services
  - Review your system’s plans, policy, and architecture
  - Provide data privacy and security guidance and advice
  - Provide technical security analysis to improve and fine-tune your system’s security posture, implement best practices, and provide that all-important “third party perspective”
  - Create and deliver customized data privacy and security awareness training
PTAC Assistance – Rapid Response

- PTAC is ready to help in responding to privacy and security incidents
  - Provide real-world guidance and advice on response activities
  - Lend advice and help supplement technical staff in conducting investigation activities
  - Help organizational decisionmakers determine a strategy for recovery
Security Resources

- DHS United States Computer Emergency Response Team (US-CERT) - [https://www.us-cert.gov/](https://www.us-cert.gov/)
Contact Information

Family Policy Compliance Office
Telephone: (202) 260-3887
Email: FERPA@ed.gov
FAX: (202) 260-9001
Website: familypolicy.ed.gov

Privacy Technical Assistance Center
Telephone: (855) 249-3072
Email: privacyTA@ed.gov
Fax: (855) 249-3073
Website: ptac.ed.gov