IT Security Update

February 24, 2017

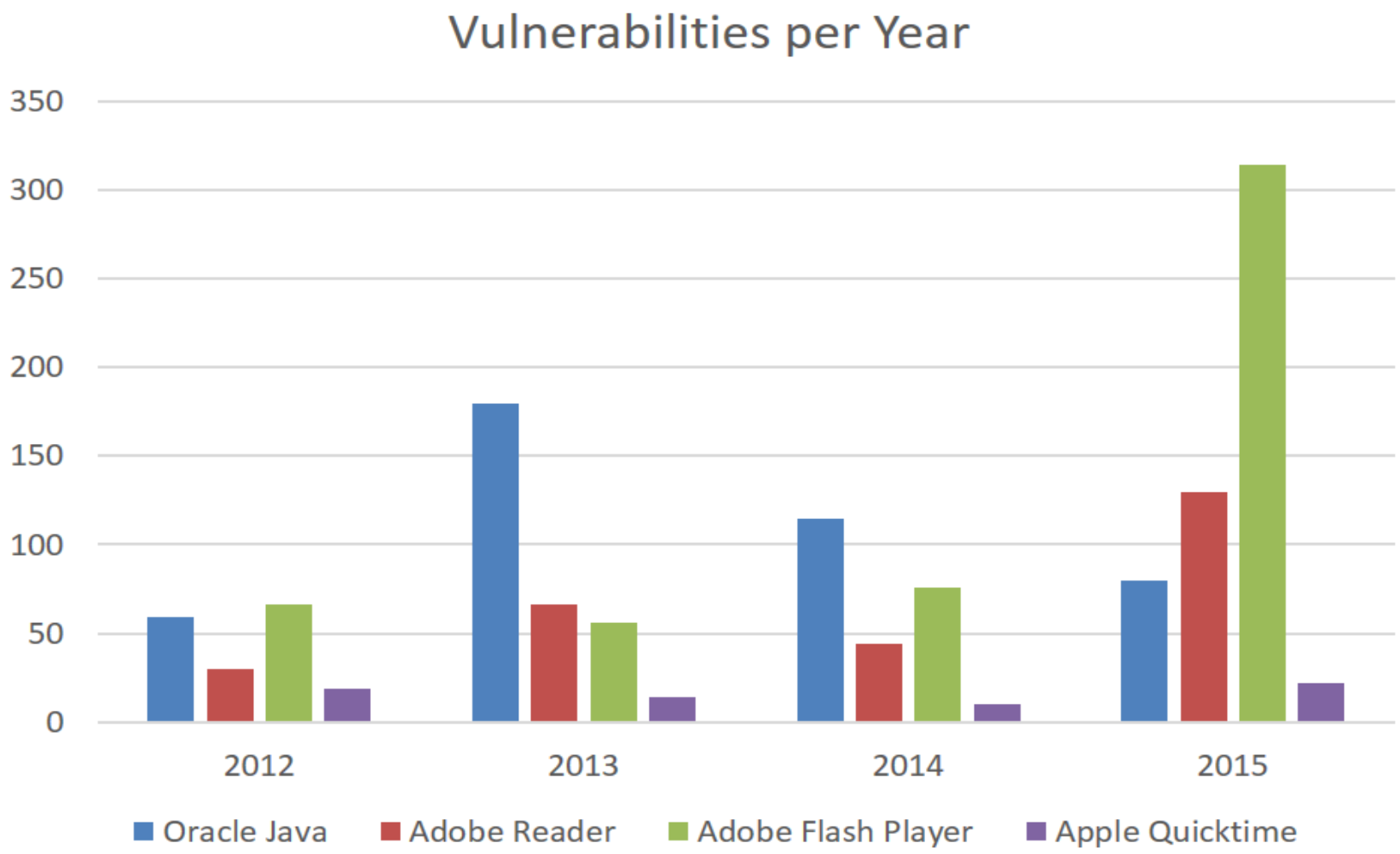
Terry Overton, Information Security Officer, Information Services Division

2014 – Where We Left Off

- Last Report – FEB 2014
  - Progress update on remediation of Intrinium Findings
  - New Information Security Officer (ISO) introduced
  - Annual Security Awareness Training implemented
- Security Strategy Development
  - New security model chosen (SANS Top 20)
  - Critical risks identified and prioritized
  - ISO assessments required for new and ongoing projects
- New Tools & Processes
  - JIS Data Classification Standard Adopted (NOV 2014)
  - New Tools: Vulnerability Scanner, Network Access Control, Automated Patch Management Tool, Web App Firewall

2015 – Putting the Pieces in Place

- Hired (full-time) Network Security Analyst
  - Expert in vulnerability detection and remediation
  - Assisted in deployment and configuration of new tools
  - Automated processes for rapid deployment of patches
- Appellate Courts Security Assessments
  - Marks completion of AOC enterprise security assessment
  - Scaled down version of AOC core assessment
  - Remediation efforts started quickly
- Security Initiatives in 2015
  - Software Management process implemented
  - Standardized application assessment process integrated into projects – from conception throughout operational phases



Source: HEIMDAL Security

2016 – Moving Forward

- Hired (full-time) Application Security Analyst
  - Expert in Web Application Security
  - Working closely with project teams and new product analysis
- Completing Privilege Reductions at AOC
  - Removing admin privileges from non-administrators
  - Preparation begun with Appellate administrators
    - Goal is to complete entire enterprise by end of second quarter 2017
- Exploring Options for Secure Collaboration Solutions
  - Testing of 'BOX' file-share solution – reviewing results
  - Tracking progress and trends in other state agencies
  - Working with Microsoft to evaluate their offerings in this space

2017 – Adjusting to the Threatscape

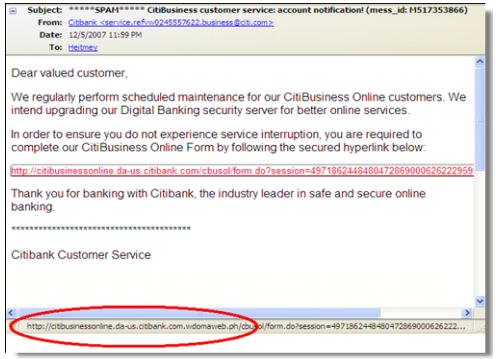
- The Basics Haven't Changed
  - Phishing exploits initiate nearly all successful intrusions
  - Unpatched software enables most attacks
  - Excess privileges make hacks easier and more effective
  - Weak and stolen credentials are still 'keys to the kingdom'
    - Multifactor Authentication is rapidly becoming the new standard
- Cyber Criminals Have Organized
  - Established crime families, as well as new players
  - Ransomware costing agencies and businesses billions
  - Controlling access to data is more important than ever
- Cyber Criminals Only Win When We Help
  - Trained workforce ***still*** the best defense against cyber criminals

Looking Forward

- Early Detection and Risk Avoidance
  - Finding weak credentials before they're exploited
  - Leveraging detailed logs to spot anomalous behavior
  - Moving away from browser plugins that cripple security
- Enhancing Incident Response Plan (IRP)
  - Work has begun on an expanded IRP
  - AOC Disaster Recovery program is 'top shelf'; IRP will follow this lead
- Continue to Automate Security Assessments
  - Project leads become familiar security inputs
  - Security requirements are anticipated, reducing surprises
  - Produces more secure, less expensive product
    - Security is cheaper & less intrusive when it's 'baked in', instead of tacked on

2016 Verizon Breach Report

- More people are opening and clicking on phishing emails than ever before.
  - Up 30% from last year


Subject: *****SPAM***** CitiBusiness customer service: account notification! (mess_id: H517353866)
From: Citibank <service.refno02455557622.business@citi.com>
Date: 12/5/2007 11:59 PM
To: Helmez

Dear valued customer,

We regularly perform scheduled maintenance for our CitiBusiness Online customers. We intend upgrading our Digital Banking security server for better online services.

In order to ensure you do not experience service interruption, you are required to complete our CitiBusiness Online Form by following the secured hyperlink below:

http://citibusinessonline.da-us.citibank.com/cbusol/form.do?session=4971862448480472869000626222959

Thank you for banking with Citibank, the industry leader in safe and secure online banking.

****

Citibank Customer Service

http://citibusinessonline.da-us.citibank.com.vidomaweb.ph/cbusol/form.do?session=4971862448480472869000626222...

- Credentials are the most coveted prize.
  - 63% of the confirmed data breaches in 2015 involved leveraging stolen passwords.
- The majority of data breaches begin with a phishing campaign.

Contact Info:

- **Terry Overton**
- Information Security Officer
- Administrative Office of the Courts
- Information Services Division
- **360.704.5500**
- Terry.overton@courts.wa.gov