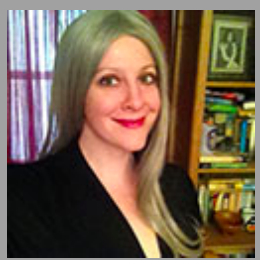
Attacks/Breaches

12/28/2015
06:00 PM



Sara Peters
News

Connect

15 Cybersecurity Lessons We Should Have Learned From 2015, But Probably Didn't

Another infosec year is almost in the books. What did all the breaches, vulnerabilities, trends, and controversies teach us?

As is the case every year in the cybersecurity field, 2015 was full of lessons to be learned. Some brand new, others that it's absurd we haven't learned yet.

1. Pay For Your Room In Cash.

Retailers were in hit hard in 2014, but in 2015 point-of-sale hacks really moved over to the hospitality sector. Just Thursday, Hyatt Hotels announced it was the last to be breached (it had discovered the incident Nov. 30). Before that Hilton Worldwide, Mandarin Oriental, and Starwood Hotels & Resorts (the owner of Sheraton, Westin, and W Hotels) all suffered breaches due to similar attacks. It isn't just credit card data that is appetizing to attackers either. Info about loyalty programs is hot on the black market too.

2. Take The Train Instead.

This was the year when car hacking really got taken seriously. Security researchers Chris Valasek and Charlie Miller conducted a controversial demonstration taking remote control of a Jeep Cherokee and bringing it to a screeching stop. The Virginia State Police showed their cruisers could be compromised and researchers showed SMS messages sent to insurance dongles can kill brakes on cars. The issue got so unavoidable that Chrysler recalled 1.4 million vehicles and Intel founded a Car Security Review Board.

3. Trust Apple, But Not As Much.

Although security researchers agree that the state of Apple security is still far better than Android, but the trusted development environment took some serious hits this year. XCodeGhost snuck Trojanized iOS apps into the official App Store, a variety of proof-of-concept exploits in Gatekeeper allow unsigned code to run on OS X, and malware for iOS and Mac is increasing.

4. The Encryption Backdoor Debate Is Not Going Away.

The U.S. intelligence agencies may have retreated periodically -- backing off on demands for encryption backdoors, and focusing its wrath instead on end-to-end encryption -- but that doesn't mean the conversation is over. With every new terrorist act, the threat of having liberties and privacy taken away becomes greater, and the encryption discussion has even become part of Presidential debates.

5. Don't Get Sick.

Over the past 10 years, more than one-quarter of reported data breaches happened in the healthcare industry, according to Trend Micro. This year, the PHI exposures at medical insurers were of gobsmacking dimensions -- 10 million records exposed by Excellus Blue Cross Blue Shield (BCBS), 11 million by CareFirst BCBS, 11 million by Premera BCBS, 250,000 by LifeWise, and a stomach-turning 80 million from Anthem Healthcare.

6. Exporting Exploits and Hoarding 0-Days Are Bad...Unless You're A Government.

Proposed updates to the Wassenaar Arrangement this year (which are getting another look, thanks to the advocacy efforts of security professionals) would put tight restrictions on US companies' ability to export "intrusion software" internationally. Yet, the breach of Italian surveillance company Hacking Team revealed that many government agencies, including the U.S.'s FBI, purchased surveillance, exploit tools, and zero-day vulnerabilities from the firm. An FBI official recently publicly admitted that the Bureau buys zero-days and the NSA says it discloses 90 percent of the vulnerabilities it finds, but not how quickly it does so.

7. Flash Will Survive The Apocalypse.

Adobe Flash has been riddled with critical vulnerabilities this year, including some zero-days revealed in the Hacking Team leaks. US-CERT released an advisory, Mozilla stopped running Flash by default, and Facebook's security chief demanded Adobe announce a date of-death for Flash. Yet, the technology persists. So, Flash is in the same category as cockroaches and ticks. Everyone wants them to die, but try as they might, they just can't kill them. So, really, if you want your manifesto to still be viewable after the collosal supervolcano or sentient robot uprising, build it in Flash.

8. Government Jobs Aren't Really So 'Secure'.

The breach at the U.S. Office of Personnel Management resulted in the exposure of personal data on anyone who's had a background check via OPM going back to the year 2000. In all, 21.5 million people's Social Security numbers, residency and employment history, family, health, and financial history as well as fingerprints on 5.6 million people were exposed.

9. Keep Backups. No, Really.

Ransomware was everywhere in 2015, and there's no reason to expect its growth will stop or slow down. Research found that ransomware use was growing, the malware itself was growing more sophisticated, the business models were becoming more varied, it had an exceptionally high return on investment, and many targets were helpless against it. Even several police departments simply paid up when they couldn't recover their assets any other way.

10. Extortionists Have More Than Ransomware At Their Disposal.

In addition to the criminals using ransomware to extort mpney from victims, there are bad guys gathering their Bitcoins from DDoS, doxing, or other cyber-enhanced blackmail threats. The Ashley Madison breach gave extortionists, blackmailers, and the average unscrupulous capitalist plenty of opportunities to collect.

11. Manage Privileged Users Better.

Study, after study, after study this year revealed that privileged accounts need to be better managed. It isn't just that the credentials themselves are too weak but sometimes they're poorly monitored, too widely shared, and they're not efficiently revoked when employees leave an organization.

12. Watch Out For Insiders.

Another reason to manage privileged accounts is that not all who are privileged are trustworthy. 2015 kicked off with news that Morgan Stanley fired a wealth advisor who accessed data on about 10 percent of its client roster and publicly posted details for 900 of them online.

13. Start Making Friends at the FTC.

The Third U.S. Circuit Court of Appeals ruled that the U.S. Federal Trade Commission could move forward with its lawsuit that alleged Wyndam Worldwide hotel chain should be held responsible for leaving its customer data unprotected. The ruling effectively gives the FTC the power to regulate the security practices of businesses.

14. Everyone Could Be A Target Of Cyber-espionage.

Whether it's the St. Louis Cardinals hacking the Houston Astros, cybercriminals attacking Kaspersky Lab to stay ahead of their threat intelligence, or operators of a shadowy illegal online gambling business hacking their third-party software provider to make sure their work for a competing gambling company wasn't a threat to their business, the takeaway is, cyber-espionage can happen to anyone.

15. Beware The Thing.

Cars and drones, Fitbits and smart fridges, baby monitors and Hello Barbie, satellites and smart cities...security vulnerabilities were found all over the Internet of Things this year. The coolest hacks this year were all at that intersection between the physical and the virtualm and the FBI even came out with a warning about the cybersecurity risks of IoT devices. Luckily, new organizations are arising to try to fix IoT security before it gets completely out of hand.

Sara Peters is Senior Editor at Dark Reading and formerly the editor-in-chief of Enterprise Efficiency. Prior that she was senior editor for the Computer Security Institute, writing and speaking about virtualization, identity management, cybersecurity law, and a myriad ... View Full Bio

Live Events Webinars

Latest Comment: At least they offer discretion for relationships :D

Cartoon Archive

Current Issue

E-Commerce Security: What Every Enterprise Needs to Know

The mainstream use of EMV smartcards in the US has experts predicting an increase in online fraud. Organizations will need to look at new tools and processes for building better breach detection and response capabilities.

Download This Issue! Subscribe Now!

Back Issues | Must Reads

Flash Poll

What's missing from your incident response plan? (Pick all that apply.)

- Access to activity logs
- An up-to-date network diagram
- Blueprint for public disclosure
- Hostname-IP address maps
- IR fire drills before the event

- [ ] Plan for finding malicious files after the breach
- [ ] We don't have an incident response plan
- [ ] Other (Please explain in the comments)

Submit

All Polls

Slideshows

Tech Gifts That Security Pros Will Probably Return

0 comments | Read | Post a Comment

2015 Ransomware Wrap-Up 3

10 Funny Twitter Feeds For Security Geeks 4

More Slideshows

Twitter Feed

F5 Networks Security @F5Security 2h
"9 coolest #hacks of 2015" oak.ctx.ly/r/455s3 via @DarkReading
Show Summary

RobertCruz03 @RobertCruz03 3h
15 #Cybersecurity Lessons We Should Have Learned From 2015, But Probably Didn't darkreading.com/attacks-breach… via @DarkReading
Retweeted by Eric Vanderburg
Show Summary

RobertCruz03 @RobertCruz03 3h
15 #Cybersecurity Lessons We Should Have Learned From 2015, But Probably Didn't darkreading.com/attacks-breach… via @DarkReading
Show Summary

SuperiorReview @SuperiorReview 13h
How 'Digital Forensic Readiness' Reduces Business Risk via @darkreading buff.ly/1NyOeoO
Retweeted by Phillip Cassady

Bug Report

Enterprise Vulnerabilities
From DHS/US-CERT's National Vulnerability Database

- CVE-2013-7445
  Published: 2015-10-15
  The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated b...

- CVE-2015-4948
  Published: 2015-10-15
  netstat in IBM AIX 5.3, 6.1, and 7.1 and VIOS 2.2.x, when a fibre channel adapter is used, allows local users to gain privileges via unspecified vectors.

- CVE-2015-5660
  Published: 2015-10-15
  Cross-site request forgery (CSRF) vulnerability in eXtplorer before 2.1.8 allows remote attackers to hijack the authentication of arbitrary users for requests that execute PHP code.

- CVE-2015-6003
  Published: 2015-10-15
  Directory traversal vulnerability in QNAP QTS before 4.1.4 build 0910 and 4.2.x before 4.2.0 RC2 build 0910, when AFP is enabled, allows remote attackers to read or write to arbitrary files by leveraging access to an OS X (1) user or (2) guest account.

- CVE-2015-6333
  Published: 2015-10-15
  Cisco Application Policy Infrastructure Controller (APIC) 1.1j allows local users to gain privileges via vectors involving addition of an SSH key, aka Bug ID CSCuw46076.

Dark Reading Radio

Archived Dark Reading Radio

The Cybersecurity Year In Review

In this end-of-the-year special edition of Dark Reading Radio, Black Hat general manager Steve Wylie and MACH37 general partner Bob Stratton will join Dark Reading editors Tim Wilson, Sara Peters and Kelly Jackson Higgins, to discuss the highlights (and lowlights) of 2015.

FULL SCHEDULE | ARCHIVED SHOWS