Security in an Age of Zero Trust

Jon Oberheide
CTO, Duo Security, Inc.
Bad week for security :(

#!/bin/bash

NSS

Xen

jQuery

Amazon Web Services
Introduction

● Who?
  ○ Jon Oberheide
  ○ CTO, Duo Security
  ○ Reformed(?) hacker, self-loathing academic, person

● What?
  ○ Some nonsense^Winsight on security trends
  ○ This is a meta-deck, lots of links!
Not-so-surprising trends

- **Cloud**
  - 2009: 3% implemented, 9% planning
  - 2013: 36% implemented, 46% planning

- **Mobile**
  - BYOD: > 286M workers
  - > 83% chose their own device

Not-so-surprising trends

Security Forcing Functions – Mobility & BYOD

By 2017, 50% of employers will require you to BYOD\(^2\) for work.

By 2018, 25% of enterprise traffic will flow directly mobile-to-cloud.\(^3\)

Smartphones: 58%

Tablets: 42%

http://www.slideshare.net/x509v3/scale-vp-wisegateinvestinginsecurityinnovationaug2014gartnercatalyst
Changes in IT environments

As users go mobile and services go to the cloud, a perimeter-less IT model means a loss of control.

IT 1.0: Mainframe  
IT 2.0: Client/Server  
IT 3.0: Cloud/Mobile
IT “evolution”? NO!

SAVE YOURSELF MAMMAL! WE WILL FEND OFF THE ASTEROIDS!
What’s new in IT 3.0?

● Users
  ○ Access from anywhere, anyhow
  ○ “Zero Trust” environment

● Devices
  ○ Mobile proliferation
  ○ BYOD acceptance

● Services
  ○ Diminishing perimeter
  ○ IaaS, cloud apps, BYOSaaS
What’s new in IT 3.0?

● Users
  ○ Access from anywhere, anyhow
  ○ “Zero Trust” environment

● Devices
  ○ Mobile proliferation
  ○ BYOD acceptance

● Services
  ○ Diminishing perimeter
  ○ IaaS, cloud apps, BYOSaaS

Hooray Productivity!
What’s new in Sec 3.0?

● Users
  ○ Access from anywhere, anyhow
  ○ “Zero Trust” environment

● Devices
  ○ Mobile proliferation
  ○ BYOD acceptance

● Services
  ○ Diminishing perimeter
  ○ IaaS, cloud apps, BYOSaaS

Emergence of mobile threats
Phishing, credential theft, etc
Limited endpoint control
Loss of visibility and control
Security by contract
User-targeted attacks
Security challenges in IT 3.0

A loss of control precludes the deployment of most traditional security controls in an IT 3.0 environment. Security must move up the stack, just as attackers have.
Where are our current controls?

- AV/HIDS
- FW/IDS/IPS
- DLP
- WAF
- SIM/SEM
- DB/DAM
- Data protection

Diagram:

- Behavior
- Users
- Devices
- Applications
- Servers
- Data
Case study: Salesforce on mobile

How do you protect this environment?
What are security vendors saying?
Cisco?

http://www.rsaconference.com/events/us14/agenda/sessions/1344/stop-looking-for-the-silver-bullet-start-thinking
Qualys?

http://www.rsaconference.com/videos/127/the-cloud-security-nightmare-or-our-next-great
Symantec?

Antivirus pioneer Symantec declares AV “dead” and “doomed to failure”

Company concedes AV fails to catch majority of malicious attacks in circulation.

'Antivirus is dead? If you think that's news, you've been living in a different world'

Summary: With the continuing rise of cloud services, security execs have been proclaiming the death of antivirus software. But, according to F-Secure, the security is not so much dead as changed beyond all recognition.
At a high level

- Market speak
- Nexus of forces
- Product positioning
- Vendors at 50k ft altitude
But I’m afraid of APT!?!
APT?
APT?

Actually Pretty Tame
APT?

Average Phishing Technique
Not so advanced

- Phishing against HVAC supplier
- HVAC -> Target corporate network
- Default credentials on internal systems
- POS malware written by Russian teenager
- Exfiltration over _FTP_
Who’s to blame?

Target, orrrr...the industry?

Target, PCI Auditor Trustwave Sued By Banks

Trustwave apparently certified the retailer as PCI compliant -- but can PCI assessors be held liable for data breaches?

The security firm Trustwave and the retailer Target have both been named in a lawsuit that claims the company's data breach was due to its PCI non-compliance.

Clean reviews preceded Target's data breach, and others

Article by: JENNIFER BJORHUUS, Star Tribune  |  Updated: March 31, 2014 - 9:27 AM

Critics say company that assessed Target has been sloppy in past.
Who’s to blame?

Target, orrrr...the industry?
Who’s to blame?

Target, orrrr... the industry?

Target did not respond to FireEye security alerts prior to breach, according to report

Target might have been a tad negligent when it came to observing its security systems last year, according to a report published March 13, 2014 by Forbes.com.

Target’s publicity relations division could not be immediately reached for comment on the report.

The report says that FireEye, a security firm, notified Target over the phone of a possible security breach a few days prior to December 2013. The report states that FireEye had been monitoring Target’s systems for three months prior to this phone call.

The report, which cites sources “familiar with the breach,” claims that FireEye’s alert was not enough to stave off a massive data breach at Target, which resulted in the theft of sensitive customer information and further investigations into the cause of the data leak.
Who’s to blame?

Target, orrrr...the industry?

Target did not respond to FireEye security alerts prior to breach, according to report

March 13, 2014

Target might have been a tad negligent when it came to observing its security systems last year, according to FireEye research.
Alarming results

- Simple attacks succeed at an alarming rate
- Attackers are going after users and their access
- Lack of focus on security fundamentals

What are progressive companies doing?
Google - Beyond Corp

Vision: Access
No "Perimeter"
Authentication
Authorization
Encryption

https://www.usenix.org/conference/lisa13/enterprise-architecture-beyond-perimeter
Google - Beyond Corp

Vision: User Experience
work from anywhere
cloud based workflows
limit access by policy only

https://www.usenix.org/conference/lisa13/enterprise-architecture-beyond-perimeter
Netflix - 100% cloud

10X Goal for 2014

100% of Corporate IT in SaaS/Public Cloud

“Sounds great, but how do we accomplish this?”

http://www.slideshare.net/mdkail/it-ops-2014-technology-roadmap
Netflix - 100% cloud

Identity Is The New Perimeter

- ZERO TRUST NETWORK ARCHITECTURE
  - CORE NETWORK STABILITY IS PRIORITY #1
  - ARUBA 802.11AC UPGRADE
  - VPN REQUIRED TO DC FROM EVERYWHERE
  - CERTIFICATE-BASED AUTH TO NIGHTMARES
    - EJBCA
    - ARUBA CLEARPASS

http://www.slideshare.net/mdkail/it-ops-2014-technology-roadmap
$50B+ financial provider

Tearing out their SSL VPN
  ○ An “enterprise network” is now an abstract idea

Tearing out their MDM
  ○ Not culturally-compatible with consumerized IT

Define lightweight, consistent access security policies across devices and services
Progressive companies

- These companies see the writing on the wall and are getting ahead of the curve

- Similarities
  - Embracing cloud and mobile
  - Assuming a zero trust environment
  - Anchoring on user and device authentication
  - Protecting user access
What should I do?
I’m not Google, Netflix, or <redacted>!
Panic?

Totally valid coping mechanism
Rejection

“That would never work for my org!”
Blind acceptance

“I’m burning down my datacenter tomorrow.”
Recognize the changing role of IT

● Previously
  ○ **User:** “Can I ...?”, **IT:** “No.”

● Then
  ○ CEO shows up with shiny new iPad
  ○ Employees spinning up SaaS applications left and right

● Now
  ○ **IT:** “How can partner with my users so they'll actually ask?”
  ○ “Department of No -> Department of Secure Enablement”
Keep an open mind

- Digest (breakfast and thoughts)
- Keep an open mind throughout the day
- Watch some of the linked content later
- Think a little further out, beyond the headlines

- Enjoy the event!