Security in an Age of Zero Trust

Jon Oberheide
CTO, Duo Security, Inc.
Introduction

- **Who?**
  - Jon Oberheide
  - CTO, Duo Security
  - Reformed(?) hacker, self-loathing academic, person
  - Previously UofM, Arbor, Merit, other MI thingies

- **What?**
  - Some nonsense^ Winsight on security trends
  - WTF is “Zero Trust”?
Not-so-surprising trends

- **Cloud**
  - 1.5 trillion in IT spending
  - 2009: 3% implemented, 9% planning
  - 2013: 36% implemented, 46% planning

- **Mobile**
  - BYOD: > 286M workers
  - > 83% chose their own device
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 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 infrastructure, SaaS/cloud apps
What’s new in IT 3.0?

- Users
  - Access from anywhere, anyhow
  - “Zero Trust” environment
- Devices
  - Mobile proliferation
  - BYOD acceptance
- Services
  - Diminishing perimeter
  - IaaS infrastructure, SaaS/cloud apps

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 infrastructure, SaaS/cloud apps

Related terms:
- User-targeted attacks
- Emergence of mobile threats
- Limited endpoint control
- Loss of visibility and control
- Security by contract
- Phishing, credential theft, etc
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?
It’s been a (not-so) good run
AV is dead?

Antivirus pioneer Symantec declares AV “dead” and “doomed to failure”
Company concedes AV fails to catch majority of malicious attacks in circulation.

by Dan Goodin - May 5 2014, 12:25pm

Commercial antivirus pioneer Symantec, in a rare admission of defeat, has conceded that antivirus (AV) software is dead.

 antivirus pioneer Symantec declares AV “dead” and “doomed to failure”
Company concedes AV fails to catch majority of malicious attacks in circulation.

by Dan Goodin - May 5 2014, 12:25pm

Commercial antivirus pioneer Symantec, in a rare admission of defeat, has conceded that antivirus (AV) software is dead.

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.
What are security vendors saying?
Symantec?

HP?

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

Qualys?

http://www.rsaconference.com/videos/127/the-cloud-security-nightmare-or-our-next-great
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
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 an agreement making claims against the company publicly.

Clean reviews preceded Target's data breach, and others

Article by: JENNIFER BJORHUS, 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?

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 lawsuits stemming from the recent data breach.

Clean reviews preceded Target's data breach, and others

Article by: JENNIFER BJORHUS, 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?

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.

Share this article:  
Share

March 13, 2014

Adam Greenberg, Reporter

Follow @writingadam
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 Re/Source Intelligence. The company’s senior advisor says that FireEye’s alert was sent to Target’s executives in early January last year but the company missed it due to its systems not being properly configured. The alert was also sent to Target’s security team, who failed to take action. The company’s management then asked the incident response team to investigate the alert, but it was too late. The investigation found that the malware used in the breach had already been detected by a signature scan, but the alert was not triggered because the system was not configured to do so.
Alarming results

- Simple attacks are succeeding at an alarming rate
- Attackers are going after users and their access
What are progressive companies doing?
Google - Beyond Corp

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
Facebook - Protect the graph

Protecting a billion identities
Without losing (much) sleep

Mark Crossbie, Four Flynn, Tim Tickel
Facebook Security Team

http://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/index/d3676r45gc9eir0n1k7u29m0hk
Facebook - Protect the graph

http://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/index/d3676r45gc9eir0n1k7u29m0hk
Progressive companies

● These companies see the writing on the wall
● 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, Facebook, or Netflix!
Panic?

Totally valid coping mechanism
Rejection

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

“I’m burning down my datacenter tomorrow.”
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 conference!
Questions?

Q & A

Jon Oberheide
@jonoberheide
jono@duosecurity.com