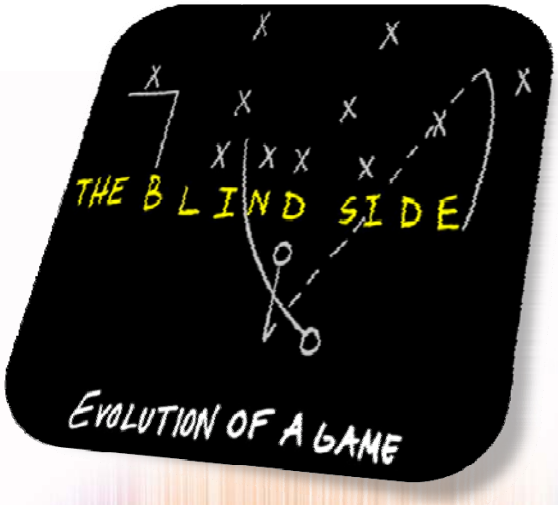
QuestNet 2011
14 July 2011

The IT Blind Side

Andrew Latham
Senior Systems Engineer



IT SECURITY & COMPLIANCE AUTOMATION


SQL INJECTION
MALWARE
A THIEF
PRIVILEGED USER
19
2
64


TOUCHING WIRES CAUSES
INSTANT DEATH
$200 FINE
Newcastle Tramway Authority

What Needs To Change?

Configurations Don't Lie

A Look At Breaches

What commonalities exist?

- **83%** of victims were targets of opportunity (<>)
- **92%** of attacks were not highly difficult (+7%)
- **76%** of all data was compromised from servers (-22%)
- **86%** were discovered by a third party (+25%)
- **96%** of breaches were avoidable through simple or intermediate controls (<>)
- **89%** of victims subject to PCI-DSS had not achieved compliance (+10%)

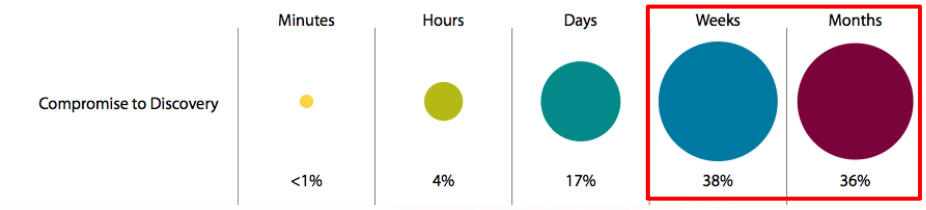
Source: Verizon Business 2011 Data Breach Investigations Report

IT SECURITY & COMPLIANCE AUTOMATION

tripwire TAKE CONTROL.

Time Span of Breaches

Figure 37. Timespan of events by percent of breaches



Source: Verizon Business 2011 Data Breach Investigations Report

IT SECURITY & COMPLIANCE AUTOMATION

tripwire TAKE CONTROL.

PCWorld

Microsoft Data Breach Heralds Things to Come

By Keir Thomas, PCWorld
December 23, 2010

What might be the first major cloud data breach happened Wednesday. Microsoft announced that ***data*** contained within its Business Productivity Online suite (BPOS) has been ***downloaded by non-authorized users.***

The knee-jerk reaction might be to blame hackers, but that's not so here. ***The breach was down to an unspecified "configuration issue"*** in Microsoft's data centers in the United States, Europe and Asia. The Offline Address Book component of BPOS, which contains business contact information, was made available to non-authorized users in "very specific circumstances," according to Clint Patterson, the poor guy at Microsoft who's having to apologize for the mistake.

tripwire TAKE CONTROL.

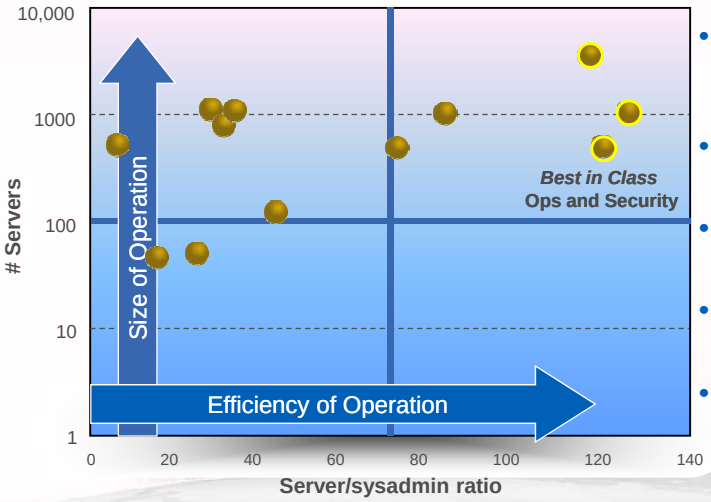
Best practices of high performing IT organizations

Seven practical steps to go from "good to great"

tripwire TAKE CONTROL.

Desired Outcome: Create A Higher Performing, More Nimble and More Secure IT Organization

Operations Metrics Benchmarks:
Best in Class: Server/sysadmin ratios



- Highest ratio of staff for pre-production processes
- Lowest amount of unplanned work
- Highest change success rate
- Best posture of compliance
- Lowest cost of compliance

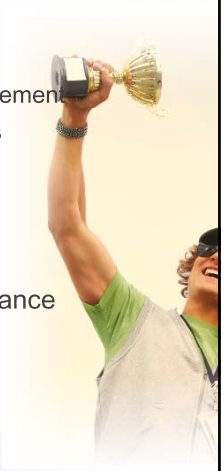
Source: IT Process Institute

Where Did The High Performers Come From?

Common Traits of the Highest Performers

Culture of…

- Change management
  - Integration of IT ops/security via problem & change management
  - Processes serving both org needs and business objectives
  - Highest rate of effective change
- Causality
  - Highest service levels (MTTR, MTBF)
- Compliance and continual reduction of operational variance
  - Production Configurations
  - Highest level of pre-production staffing
  - Effective pre-production controls
  - Effective pairing of preventive and detective controls



IT SECURITY & COMPLIANCE AUTOMATION
Source: IT Process Institute

tripwire TAKE CONTROL.

Three Controls Predict 60% Of Performance

To what extent does an organization define, monitor and enforce the following?

1. Standardized configuration strategy
2. Controlled access to production systems
3. Process discipline and accountability

Source: IT Process Institute, May 2008

IT SECURITY & COMPLIANCE AUTOMATION

tripwire TAKE CONTROL.

Visible Ops: Playbook of High Performers

IT Process Institute
Research | Benchmarking | Prescriptive Guidance

- The IT Process Institute has been studying high-performing organizations since 1999
  - What's common to all the high performers?
  - What's different between them and average / low performers?
  - How did they become great?
- Answers have been codified in the Visible Ops Methodology

IT SECURITY & COMPLIANCE AUTOMATION

tripwire TAKE CONTROL.

Seven Practical Steps

- Step 1: Gain situational awareness
- Step 2: Reduce and monitor privileged access
- Step 3: Define and enforce configuration standards
- Step 4: Integrate and enforce change management processes
- Step 5: Create library of trusted builds
- Step 6: Integrate into release management
- Step 7: Ensure that all activities go through change management

IT SECURITY & COMPLIANCE AUTOMATION

tripwire TAKE CONTROL.

Step 1: Gain Situational Awareness

- Situational awareness: “the ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regard to the mission.”
- Find Fragile Artifacts

ON

tripwire TAKE CONTROL.

Step 2: Reduce And Monitor Privileged Access

- Look for admins with high levels of privilege
  - Question the need for elevated privileges
  - Reduce access, strictly control who can log in with “super powers”
- Implement preventive controls:
  - Reconcile admins to authorized staff and delete any ghost accounts
  - Issue and revoke accounts upon hiring, firing, reassignment
- Implement detective controls:
  - Monitor privileged user account adds, removes and changes
  - Reconcile each user account change to an authorized work order
  - Implement account re-accreditation procedures

“To err is human. To really screw up requires the root password.”
—Unknown

Step 3: Define And Enforce Configuration Standards

Step 3: Define And Enforce Configuration Standards

- The goal is to create known, trusted, stable, secure and risk-reduced configuration states
- External configuration guides include:
  - Center for Internet Security (CIS)
  - Defense Information Systems Agency (DISA) STIGs
  - Vendor Hardening Guidelines:
    - VMware: "VMware Infrastructure, Security Hardening"
    - Microsoft Hardening Guidelines

"Like their physical counterparts, most security vulnerabilities will be introduced via misconfiguration & mismanagement. Security issues related to vulnerability & configuration management get worse, not better, when virtualized.

Source: Gartner, Inc. "Security Considerations and Best Practices for Securing Virtual Machines" by Neil MacDonald, March 2007.

The Dark Side Of Virtualization

- Virtualization enables organizations to deploy changes and releases more quickly than ever
  - "What works at 60 mph may not work at 200 mph…"
- Certain required activities in the physical world made it easier to prevent and detect release risks
  - Watching for servers on the loading dock
  - Budgeting and procurement activities
  - Physical data center access
  - Network cabling

What happens when these activities are no longer required to deploy major releases?
- *And when it is easy to download VMplayer, copy virtual machines, etc…*
- *And what could go wrong?*

Step 4: Integrate & Enforce Change Management Processes

- InfoSec needs change management
  - Gain situational awareness of production changes
  - Influence decisions and outcomes
- Add value to change management by:
  - Assessing security & operational impact of changes
  - Improving procedures for change authorization, scheduling, implementation and substantiation
  - Ensuring that change requests comply with information security requirements, corporate policy, and industry standards

IT SECURITY & COMPLIANCE AUTOMATION

tripwire TAKE CONTROL.

Step 4: Integrate & Enforce Change Management Processes

- Implement preventive controls
  - Get invited to the Change Advisory Board (CAB) meetings
  - Ensure “tone at the top” and help define consequences
- Implement detective controls
  - Build and electrify the fence
  - Substantiate that all changes are authorized
  - Look for red flags and indicators

“[As auditors,] the top leading indicators of risk when we look at an IT operation are poor service levels and unusual rates of changes.” – Bill Philhower

Step 5: Create A Library Of Trusted Builds

- Goal is to make it easier to use known, stable and secure builds than unauthorized and insecure builds
- Implement preventive controls:
  - Defined process of how to assemble hardened and stable builds
  - Work with any existing server provisioning teams to add any standard monitoring agents
  - Ensure that application and service account passwords are changed before deployment
- Implement detective controls:
  - Verify that deployed infrastructure matches known good states
  - Verify that virtual image configurations against internal and external configuration standards

IT SECURITY & COMPLIANCE AUTOMATION

tripwire TAKE CONTROL.

Step 6: Integrate Into The Release Management Processes

- Release management and information security both require standardization and documentation
  - Checklists
  - Detections and reduction of variance
- Implement preventive and detective controls:
  - Develop shared templates with release management, QA and project management and integrate into their checkpoints
  - Integrate automated security testing tools
  - Compare preproduction and production images, and reduce any variance

IT SECURITY & COMPLIANCE AUTOMATION

tripwire TAKE CONTROL.

Step 7: Ensure All Activities Go Through Change Management

- Ensure that “only acceptable number of unauthorized changes is zero”
  - Infrastructure: physical and virtual
  - Application releases
  - Security patches
  - Break/fix activities
- Nobody gets a free pass
- Review and document emergency fixes
- Use automated controls to continuously monitor and enforce

IT SECURITY & COMPLIANCE AUTOMATION

tripwire TAKE CONTROL.

Higher Performing IT Organizations Are More Stable, Nimble, Compliant and Secure

- High performers find and fix security breaches faster
  - **5 times** more likely to detect breaches by automated control
  - **5 times** less likely to have breaches result in a loss event
- High performers maintain a posture of compliance
  - **Fewest** number of repeat audit findings
  - **One-third** amount of audit preparation effort
- When high performers implement changes…
  - **14 times more** changes
  - **One-half** the change failure rate
  - **10x faster** MTTR for Sev 1 outages
- When high performers manage IT resources…
  - **One-third** the amount of unplanned work
  - **8 times more** projects and IT services
  - **6 times more** applications

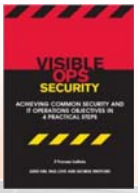
Source: IT Process Institute, May 2008

IT SECURITY & COMPLIANCE AUTOMATION

tripwire TAKE CONTROL.

How To Apply The Seven Practical Steps

- Remember the 3 highest-value controls:
  - Standardized configuration settings
  - Controlled access to production systems
  - Process discipline and accountability
- Read & apply the Visible Ops framework
- Get more information at www.itpi.org
- Visit Tripwire booth
- Get more information www.tripwire.com
- Get free Visible Ops Security Book



tripwire
TRUE CONTROL