PCI Made Simple

Craig Lawrance
XYPRO Technology
Sep 24, 2013
Agenda

- Why bother with PCI at all?
- What is happening out there in hacker-land?
- Overview of 2013 Verizon Data Breach report
- Key Security Findings and Applicability to NonStop
- Closing the Security Gaps—Securing the NonStop
About XYPRO

- Founded in 1983 – over 30 years working with the HP NonStop community
- Specialists in Mission Critical security, compliance and encryption
- Sales and Support offices around the world
- XYGATE Merged Audit & User Authentication included on all HP NonStop servers
- We wrote the book on NonStop Security—twice!
- 2013 HP Partner of the Year in Security
PCI DSS 3.0 drivers

• Card Data remains the main target

• Get the basics right
  – Weak passwords /authentication
  – Poor self-detection

• Not just an IT issue

• PCI DSS needs to become culture
Security breaches are still making news

- Yahoo Japan: 22 million logins potentially published (May 20, 2013)

- Healthcare: more than 10 breaches in May 2013

- $45 million stolen from two Middle East banks (May 9, 2013)
2013 Data Breach Investigations Report (DBIR)

- Verizon DBIR is comprehensive summary of security incidents each year
- 2013 report just published – covers incidents from 2012
  - 19 Contributors
  - 27 countries represented
  - 47,000 security incidents analyzed
  - 621 confirmed data breaches studied
  - At least 44 million compromised records
  - Many countries now looking at mandatory breach reporting laws
Verizon DBIR 2013 Overview

- **37%** of breaches affected financial institutions
- **75%** of attacks were opportunistic (majority financially motivated)
- **66%** of breaches took MONTHS OR YEARS to be identified
- **69%** of breaches identified by an external party (9% by customers!)
- **86%** of the breaches had no internal element

Source of Data Breaches
534 (86%) of the breaches that Verizon analyzed had no internal element

From 2013 Verizon Data Breach Investigations Report
Most attacks still use basic techniques

- 76% of network intrusions exploited weak or stolen credentials
- Over 78% of attack techniques were considered “low” or “very low” in difficulty (on VERIS scale)

NonStop relevance
- Implement strong user authentication
- Implement and enforce password management processes
- Enforce policy of minimum required access
- Ensure no shared super-user accounts
- Keep track of what users are doing on critical systems with key logging

From 2013 Verizon Data Breach Investigations Report

Difficulty of tactics used

- HIGH: 1 (0%)
- MODERATE: 116 (22%)
- LOW: 343 (68%)
- VERY LOW: 50 (10%)
14% of breaches were insider attacks

- Correlated - Privilege misuse weighs in at 13%
- Lax internal practices often make gaining access easier
- Over 50% of insiders committing sabotage were former employees using old accounts or backdoors not disabled
- Over 70% of IP theft cases committed by internal people took place within 30 days of announcing their resignation

- NonStop relevance
  - Ensure NonStop user provisioning is integrated with Enterprise Identity Management system
  - Enforce policy of minimum required access
  - Ensure no shared super-user accounts
  - Keep track of what users are doing on critical systems with key logging
  - Integrate NonStop with SIEM
Data at rest is most at risk

• Of 621 cases Verizon investigated, **none** involved data in transit
• 66% of breaches involved data at rest in databases and file servers (the rest was data being processed)

• NonStop relevance
  – Protect data at rest with encryption or tokenization

From 2013 Verizon Data Breach Investigations Report
Know your (potential) attacker

- Types of attack vary depending on industry and region
- Small retailers subject to attacks on poorly configured remote systems to access POS data
- Banks subjected to ATM skimming and web application attacks
- POS attacks much less frequent in Europe than AP and Americas but Retail is still the largest victim industry

- NonStop relevance
  - Based on industry/business type, protect “at risk” assets
  - Financial examples generally most applicable to NonStop users
XYPRO can help close security gaps

- **Compliance**
  - Security Policy Development
  - Configuration Monitoring
  - Compliance Alerting
  - PCI, HIPAA, SOX

- **Access Control**
  - Individual Accountability
  - Keystroke Logging
  - Privileged Access Management

- **Data Security**
  - FIPS - Validated Encryption
  - Format-Preserving Encryption
  - Tokenization
  - Masking

- **Audit**
  - Consolidated Security Data
  - Event Monitoring
  - Audit Reporting
  - Interface to SIEMs

- **Device-Centric Authentication**
  - Multi-Factor Authentication
  - Transaction Protection
  - Strong, Scalable, Transparent

- **Safeguard Management**
  - Advanced Security Admin Tools
  - Single Sign-On
  - Safeguard Audit Information

- **Database Management**
  - SQL/MX, SQL/MP, Enscribe
  - Storage Management
  - Partition Analysis
  - Monitoring and Correction Reporting

- **Identity Management**
  - Enterprise Identity & Access Management (IAM) Adaptors
  - for HP NonStop Server
XYGATE products can help

• XYGATE Password Quality (XPQ) provides all necessary support for passwords
  – Password strength, password change policies etc
• XYGATE Access Control and User Authentication remove the need for shared UserIDs, and enables role-based security
  – User impersonation allows non-super users to perform sensitive commands
  – All commands audited with the actual UserID that executed the command
XYGATE products can help

• Protecting data at rest
  – XYGATE XDP offers Format Preserving Encryption and “traditional” AES encryption options to protect all sensitive data
  – FPE can be incorporated into existing applications with no code changes via XDP

• Protect data as it is being processed
  – XYGATE Compliance PRO - ensure files & applications are not tampered with

• Integrate with SIEMs
  – XYGATE Merged Audit supports all major SIEM vendors, including HP ArcSight, and is included on the NonStop Operating System
Further Reading

• Verizon DBIR
  http://www.verizonenterprise.com/DBIR/2013/>

• Industry-specific reports
  http://www.verizonenterprise.com/DBIR/2012/verticals/>

• Mandiant M-Trends report
  https://www.mandiant.com/resources/m-trends/>

• Breach statistics
  http://datalossdb.org/
Thank you!

Craig.Lawrance@xypro.com