BEST PRACTICES FOR SECURING PRIVILEGED USERS

Presented by Brian Marshall,

Vice President, Research and Development

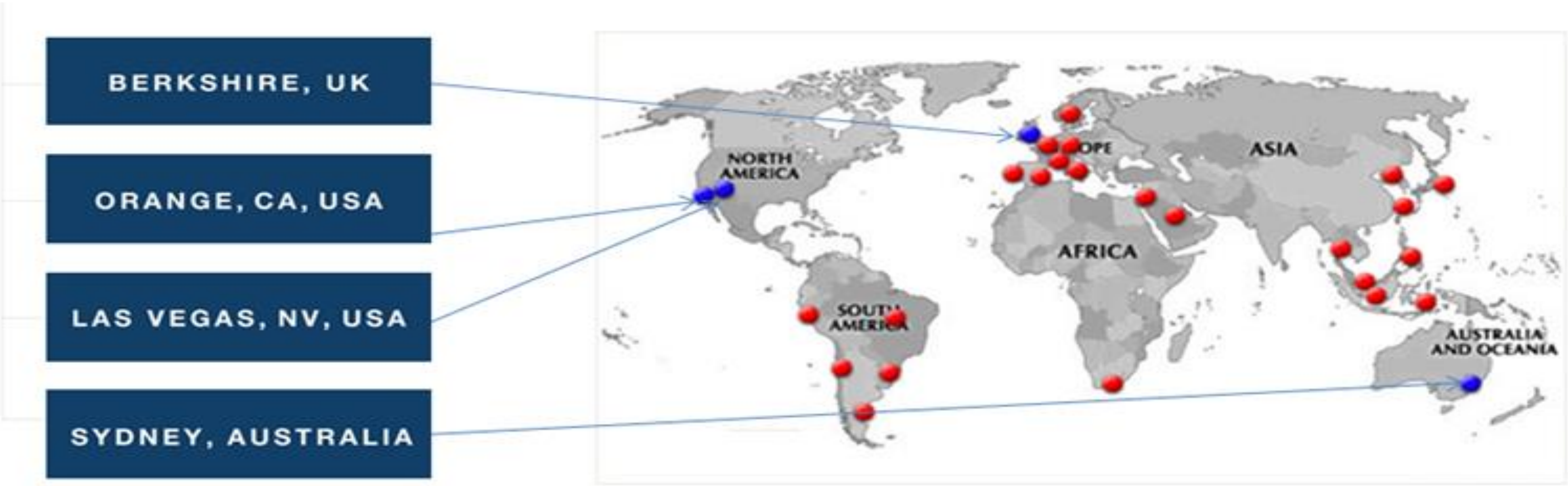
Vanguard Integrity Professionals

ABOUT VANGUARD

Founded: **1986**

Business: **Cybersecurity Experts for Large Enterprises**
Software, Professional Services,
and Training

Customers: **1,000+ Worldwide**



BERKSHIRE, UK

ORANGE, CA, USA

LAS VEGAS, NV, USA

SYDNEY, AUSTRALIA

Over 15 distributors/resellers serving 50+ countries worldwide

AGENDA

1. Scary Information on Data Breaches
2. Definition of a Privileged User (for RACF)
3. Top Ten Best Practices for Securing Privileged User Accounts
4. Questions

DATA BREACHES

- Number of breaches and outside attacks increasing

- Continuing problem of insiders - malicious or by accident

Tax Season Kicks Off with Scams
Haiti, World Cup Used to Trick
Criminals Infect Flash Drives
Cyber Crime:
Olympic Winter Games Attract Fraud
Online Crooks Romance Users with Valentine's Scams
Identity Thiefs Steal
Fake Security Software
Lured to Malicious Web Pages
Phishing Att
Hit Twit
data breach

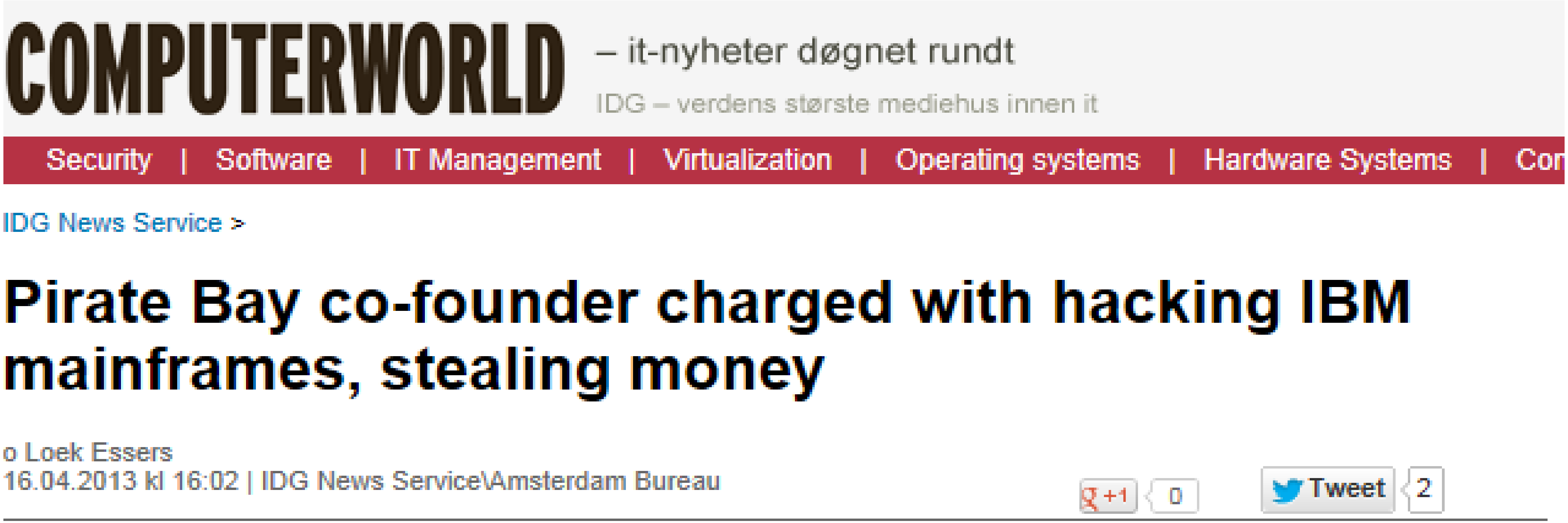
DID YOU KNOW?

“Target was certified as meeting the standard for payment card industry (PCI) in September 2013. Nonetheless, we suffered a data breach.”

> now ex-chairman, ex-president, and ex-CEO of Target Corporation, Gregg Steinhafel (bidnessetc.com, Mar. 25, 2014, Nancy Kross)

TARGET

DATA BREACHES



COMPUTERWORLD – it-nyheter døgnet rundt

IDG – verdens største mediehus innen it

Security | Software | IT Management | Virtualization | Operating systems | Hardware Systems | Cor

IDG News Service >

Pirate Bay co-founder charged with hacking IBM mainframes, stealing money

o Loek Essers
16.04.2013 kl 16:02 | IDG News Service\Amsterdam Bureau

MORE NEWS

HOME DEPOT
®

STAPLES
that was easy.sm

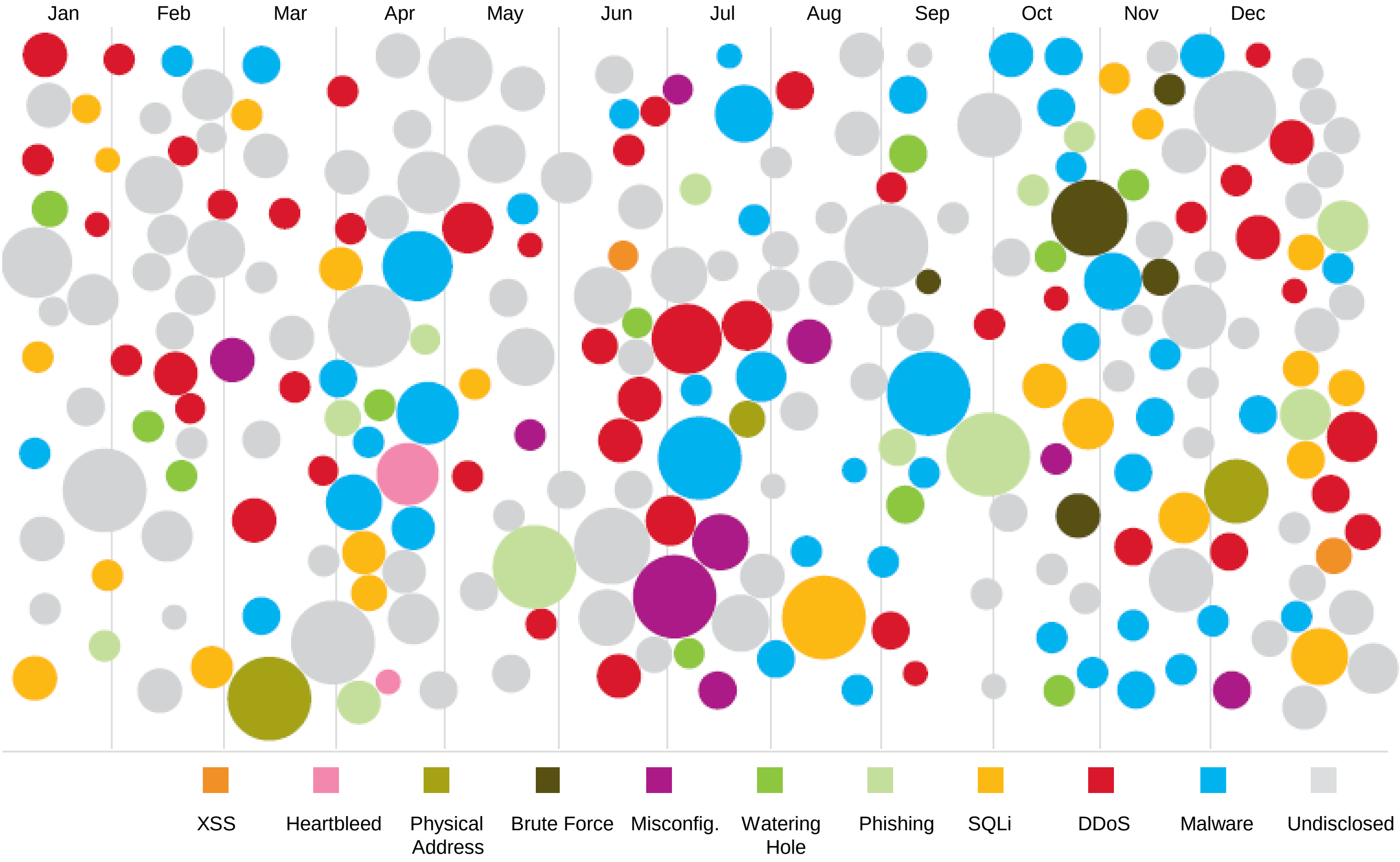
SONY
PICTURES

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
OPM.GOV

Anthem.
BlueCross BlueShield

ATTACK STATISTICS

Sampling of 2014 security incidents by attack, type, time and impact



Source: IBM X-Force Threat Intelligence Quarterly, 1Q 2015

PRIVILEGED USERS

Who or What are They?

- System and Group Special
- System and Group Operations
- UID(0)
- System and Group Auditor
- System ROAudit
- DB2 – SYSADM, SYSOPR, SYSCTRL

PRIVILEGED USERS

Who or What are They?

- **Trusted – STC users**
- **Privileged – STC user**
- **Users with APF Authorized library access GT READ**
- **All Systems Programmers**
  - Really anyone who can issue any number of MVS commands including SETPROG or SET or ….. (The list is long)

PRIVILEGED USERS

Who or What are They?

- **Users with access to:**
  - FACILITY BPX. Profiles
  - FACILITY IRR. Profiles
  - FACILITY STGADMIN. Profiles
  - UNIXPRIV SUPERUSER. Profiles
  - SURROGAT Profiles
  - OPERCMDS MVS. Profiles
  - DASDVOL Class resources
  - ISMF PROGRAM class resources
  - Any PII or PCI or Health Care Data

BASELINE YOUR PRIVILEGED USERS

- At a minimum - baseline the users that have System and Group Attributes along with UID(0) And STC users with Trusted
- No valid reason to have an STC with the Privileged attribute

USE EMERGENCY USERIDS

9

For users that otherwise would not need an authority with the exception of an emergency situation, CREATE Emergency IDs that can be checked out and passwords modified once used

SEPARATION OF DUTIES

DO NOT ALLOW users to have more than one extraordinary System or Group Attribute.

LIMIT EXTRAORDINARY USERS

- Access to multiple resources may provide the same access
- UID(0) VS BPX or UNIXPRIV
- System or Group Special Versus IRR.PASSWORD.RESET
- STC TRUSTED attribute versus understanding what an STC really needs access to
- OPERATIONS vs STGADMIN Access

RECERTIFICATION OF ACCESS AND AUTHORITY

6

On a periodic and continuous basis, every privileged user must have their privilege recertified by an authority in security and their management with justification for continued access

RESTRICTING ACCESS

- Restrict Access to Datasets and General Resources so that OPERATIONS does not provide access.

- Create a Group and connect ALL folks with OPERATIONS to this GROUP. Then permit that group to sensitive Dataset Profiles and General Resources with the level of access (Including NONE) that is desirable for these users.

PASSWORDS

- Require Complex Passwords or Passphrases
- Expire Passwords
- Keep Password Histories
- Set a Minimum Password Change Interval.

REVOKE

- Revoke due to inactivity and Remove Users in a timely manner

- Privileged users should have a shorter revoke due to inactivity and MUST be cleaned up off the system in a timely manner

AUDIT

- AUDIT, AUDIT, AUDIT and More AUDITING
- System Level Auditing for Users. SAUDIT and UAUDIT and ALL APF authorized libraries must have auditing and 14 and 15 records reviewed on an ongoing basis.

MULTI-FACTOR AUTHENTICATION

- Enforce Multi-Factor Authentication
- Human Users must be forced to use Multi-Factor Authentication. PERIOD!
- Absent Multi-Factor Authentication for ALL privileged human users, you are simply begging to be penetrated

QUESTIONS?

Don't miss the world's largest System z security training event

VANGUARD | WEST 2015
SECURITY & COMPLIANCE
SEPT 28 – OCT 1 • LAS VEGAS, NV

www.go2vsc.com

THANK YOU

Vanguard Integrity Professionals
A Company History of Innovation & Success

www.go2vanguard.com

(702)794-0014