Pillars of Incident Response: The Calm in the Storm

Brandie Anderson
Senior Manager, Global Cyber Security Production Management
Hewlett-Packard
Understand Yourself and Your Organization

http://www.netmagicsolutions.com/how-inframonitor-work
SITREP – Breach Setup

Timeline of Breach

27 Nov – Target Gets Hacked
11 Dec – Suspected date attacks discovered
18 Dec – Krebs Publishes Breach

19 Dec – Target Acknowledges the Breach
10 Jan – 70M customers added to the breach
15 Jan – $5M invested in cyber security coalition
17 Jan – Russian hackers named responsible
6 Feb – HVAC contractor identified as Hacker conduit
11 Feb – Cyber Task Force Report released

http://www.fierceitsecurity.com/node/597/print
4 Interesting Days
Dec 11 – Dec 15

Preparation
Identification
Containment
Beyond the first 4 Days

Eradication

Recovery

Lessons Learned
Trust in Your Training

Training or Experience?
eBay and PP sites breached

Whitted, Paul

To: Moody, Lucas
Cc: Black, Paul; Nguyen, Viet (NetSec); West, Scott; Fang, Michelle; Forsythe, Ralph; Patino, Juan; Stuart, Robin; Stidham, Keith; DL-Ebay-TDO-Staff@eBay.com; DL-PP-M-NOC-Group; DL-PP-M-NOC-TDO; DL-PP-dns;

Saturday, February 01, 2014 12:05 PM

Just pointing out if someone has remote access to email via compromised laptop and is on this thread then they now have our conference info to listen into this incident. Might want to have folks call into the sec / ppcc and be in breakout where password is required to join.

Paul

Sent from my iPhone
Critical Input
Remediation

Short Term

Long Term
Fundamentals

Accounts

Systems

Network
Get Help
Resources

- Investigators
- Forensics
- IT
Follow Up!
Remediation Validation

- Abnormal User Activity
- Known Bad Domain
- Tool Signature

Actionable Data
Fall Out

What good is a "communications hotline" if nobody answers the phone or calls you back? Sigh

1/31/2014 10:06:24 AM

3 RETWEETS  4 FAVORITES
Wrap Up

Understand Yourself & Your Organization

Trust Your Training

Get Help
Thank You

@ba2trinity