EVOLVING FROM BREACH PREVENTION TO BREACH ACCEPTANCE TO SECURING THE BREACH

Jason Hart  CISSP CISM
VP Cloud Solutions
Safenet Inc
Today’s issues

- Data breaches are rampant
- Data is moving everywhere
- The approach to protecting data must change
THE LEADING EDGE OF BIG DATA: THEN AND NOW
THE LEADING EDGE OF BIG DATA: THEN AND NOW
In 2000 the world generated two exabytes of new information every day.
Structured + Unstructured = BIG

Structured in Relational Databases

Telemetry, Location-Based, etc.

Internet of Things

Non-Enterprise

Managed, Unmanaged & Unstructured
Global Flight Analysis

- 60,000 Aircraft Routes
- Sensors On Each Gas Turbine Engine = 1Tb/day
Big Data Analytics: Not New

Used Already in Many Industries

- Risk Assessment
- Price Optimization
- Monte Carlo
- Regression
- Product Recommendation
Security most keep up

IT Evolution

Big Data

Cloud

Virtual

Mobile
Your Organization’s Security Professional?
Protection Requires A New Approach
Lets Start with the Basics

• Confidentiality
• Integrity
• Availability
• Accountability
• Auditability

HOW DO I ACHIEVE THIS IN A VIRTUAL WORLD?
Welcome to the next Generation

• 1\textsuperscript{st} Age: Servers
  • Servers
  • FTP, Telnet, Mail, Web.
  • These were the things that consumed bytes from a bad guy
  • The hack left a footprint

• 2\textsuperscript{nd} Age: Browsers:
  • Javascript, ActiveX, Java, Image Formats, DOMs
  • These are the things that are getting locked down
    – Slowly
    – Incompletely

• 3\textsuperscript{rd} Age: Virtual Hacking: - Simplest and getting easier
  • Gaining someone's password is the skeleton key to their life and your business
  • Accessing data from the virtual world can be simple
Virtual World – With Virtual Back Doors

Welcome to the Future

• Cloud Computing

• Virtual Environment

• With Virtual Security holes

During the past 15 years with learnt nothing
2013

SOME FACTS
Will your organization, or your partner, suffer a security breach this year?

Nobody’s immune, no target is too small, or too large.
The methods used by hackers to gain access to data are numerous, wide-reaching and ever-growing.

However Nothing Has Changed
IT’S BEST TO STICK WITH WHAT YOU KNOW

AS LONG AS WE LOCK DOWN THE NETWORK WE’LL BE SAFE, WON’T WE?
IT’S OBVIOUS WHEN YOU’VE BEEN HACKED

IT’S EASY TO SPOT WHEN SYSTEMS HAVE BEEN BREACHED, ISN’T IT?
69% of breaches were spotted by an external party — 9% were spotted by customers.

Social tactics — using email, phone calls and social networks to gain information on individuals — are often ignored, but contributed to 29% of attacks.

76% of network intrusions exploited weak or stolen credentials. Strict policies are required to reduce this easily preventable risk.
The Facts

Most breaches lie undiscovered for months...

It’s not really surprising that many breaches happen quickly — perpetrators driven by financial gain will often quickly move on if not successful. What’s alarming is how long breaches take to spot, and how long they take to fix — during which time sensitive data remains exposed.

66% of breaches lie undiscovered for months, increasing the potential damage.

Hackers are interested in companies just like yours...

All kinds of organizations — from government agencies to iconic consumer brands, internet startups to trusted financial institutions — have reported major data breaches in the last year. Nobody’s immune, no target is too small, or too large. It could be you next.

75% of attacks are opportunistic, not targeted at a specific company.

Verizon 2013 Data Breach Investigations Report
The Facts

- In 84% of cases, the initial compromise took hours — or even less.
- In 66% of cases, the breach wasn't discovered for months — or even years.
- In 22% of cases, it took months to contain the breach.

Verizon 2013 Data Breach Investigations Report

RSACONFERENCE EUROPE 2013 #RSAC
The Facts

66% of the breaches in our 2013 report took months or even years to discover (62% months, 4% years).

The problem is getting worse. In the 2012 DBIR, just 56% of breaches took a month or more to be discovered.
Threats Require A New Approach
This is about you forgetting what you know about InfoSec
You are still investing ~ 90% of your budget with the same mindset .... Into Network / Perimeter defense...
While everything around you has changed?
Just like my mother in the 60’s data was born to be free (or at least shared)
And the most scary part....
That The Problem and the ‘Solution’ are out of sync...
The new mindset ?
Transform your mind from Breach Prevention To Breach Acceptance
Finding XLS files with "password" on Amazon S3 cloud storage drives

Username and passwords for bank accounts, email, and everything else
Which means, assume a breach will happen....
Think like a bad guy...

What is he after?
Used by Hackers as a standard tool
That your perimeter (aka network) might not have died but it's not really doing well....
Ok, now what should I do?
How about ....
Kill the Data....
Kill the Data → Crypto
Is it really that simple?
SafeNet ‘Secure Breach’ Survey….

- 31% admitted that their perimeter has been breached
- 20% were not sure if they’d been breached.
- 38% believe unauthorized users currently have access to their networks.
- 65% think they will suffer a data breach within 3 years
- 59% believe if their perimeter is breached, their data would not be safe.
- 20% wouldn’t trust their own company with their personal data….
Persistent belief that perimeter defenses are effective.

Significant acknowledgement of past breaches.
Doubt in security industry’s ability to detect and prevent breaches.
Recognition that if perimeters failed, high value data would not be safe.
A new prescription for the “Secure Breach” era

Introspection
- It's time to try something new...

Acceptance
- You can’t prevent a perimeter breach...

Understanding
- Know your enemies and what they are after...

Action
- Protect What Matters...THE DATA!
Control Access To Data?
Cloud/Virtualization Loves Crypto....
Compliance Loves Crypto
High Value Data loves crypto
Hackers?
They HATE Crypto
Think breach acceptance
Data is the new perimeter

Kill The data
Kill it The Right Way
Forget Everything
InfoSec has (to) Changed
Breach Prevention?

How is that working for you?
Breach Acceptance
Accept a breach will happen
Protect What Matters
Where it matters
Breaches
Don’t like Encrypted Data

It's everywhere...
We can help
And We’ve done it before
Thank you!

Jason Hart CISSP CISM
Safnet Inc
Jason.Hart@Safenet-inc.com
www.safenet-inc.com