Lazy Security in a Large Gateway

Mark Suter, Senior Gateway Engineer

Monday, 16th January 2012

LCA 2012, Ballarat, Australia

UNISYS

Abstract

My workplace is a secure gateway for a large government client. It has many different types of devices forming a response to the risks we face in connecting to the world.

One of our largest Laziness efforts (reduce **overall** energy expenditure) is how we handle all the technical policies on all those different devices.

This talk discusses the different devices with most of the focus on what works for us, minus some detail to keep the security people onside ;)

These slides are at http://zwitterion.org/talks

Lazy?

Laziness is the quality that makes you go to great effort to reduce overall energy expenditure. It makes you write labor-saving programs that other people will find useful, and document what you wrote so you don't have to answer so many questions about it.

http://c2.com/cgi/wiki?LazinessImpatienceHubris

Security?

- Pick your favourite definition :)
- Security's **absence** or **failure** is recognisable
- Traditional definitions include:
  - Confidentiality, Integrity and Availability
  - Separation of assets and threats
  - CobiT, ISO 177799, ISO 27001, HIPPA, FISMA, PCI DSS, NIST
  - RFC 3871, **ISM**, **PSPF**, IRAP, ACSI 53
  - How to make **people** stop doing Stupid Things(TM)
- Security Theatre (perception vs actuality)

Large Gateway?

- High Profile Federal Government Client
- 238 separate pieces of hardware, 103 separate subnets
- Extensive Monitoring, Logging and Reporting
- Services include:
  - Web Browse, including content filtering and SSL intercept
  - Web Hosting, DNS, Internet Email, B2B Links and File Drop
  - Several Remote Access solutions, Lots of Firewall Management
  - IDS/IPS, Routers, Switches, Linux Servers, Anti-Virus
  - Authentication, XML Gateways, NTP, Incident Response
  - Certification Authority, Documentation, Certification

Documentation

- Our wiki
  - Dokuwiki with several tools, e.g., LIME (bespoke)
  - Single https:// website
  - All access authenticated, authorised and logged
- What do we document?
  - Continues to be the single place for **everything**
  - Be clear on what is up-to-date (modified dates, etc)
  - Increasing focuses on the “Why?” of things
- Who has access?
  - Rather wide audience (unneeded Secrecy **hurts** Security)
  - Includes the customer

Exceptions

- Every rule has an exception
  - Or maybe hundreds
  - Except, of course, this rule ;)
- Explicitly document all exceptions
  - Why it was done
  - Who approved it
  - When it should be reviewed or removed
- Check your config against for unknown exceptions

Reduce Complexity

- KISS
  - This isn't a rock band ;)
- Reality adds enough complexity without adding more
- Minimalist architectures avoid future nightmares
  - Also, they save on typing when doing documentation

Firewall Rulesets

- Recognise that firewall rulesets are **part** of security policy
  - They don't exist in isolation
  - Each rule should be implementing part of the policy
  - As much as possible, make that link explicit and written
- Document end-to-end data flows against business services
  - Automation will take care of documenting the actual rules
  - You need to know why a rule exists before changing it
  - Helps avoid unused rules you don't dare touch
- Review rules and cleanup regularly
  - Like keeping an inbox under control

Web Filtering

- We use Blue Coat Proxies
  - “Web Pulse” categories matched to Active Directory groups
- We spent a lot of effort on the error messages
  - Helps a lot with the support tickets

Training / Mentoring / Learning

- “Teach yourself” is valuable
  - Give opportunity and guidance
  - Allow “play” time
- Encourage people to learn what interests them
- Formal training has its place
  - My manager is awesome

UNISYS

Questions?

Slides at http://zwitterion.org/talks

UNISYS