

Security is HOT! Get Serious!!

Contributed by Michael Felt

Security is HOT!

Yes, that is something "we" have been saying for years. Finally, it seems that high-level business management is noticing that not securing systems and applications really does cost profit. OMG! - Securing systems is not just a bunch of Hype!

What has been going on?

My quick crystal ball (that sees perfectly into the past) tells me - while the rest of us were sleeping and having pleasant dreams - the "hacking as a business" group has done some serious study on application and platform weaknesses. And, "today" we wake from our dreams to find ourselves living a nightmare. We dreamed we were safe. Maybe better is the lesson of the fable: "The King's New Clothes"and we are at the point where the King (our business management) realizes the royal house is walking around - well, you know!

What to do now?

Regardless of whether you believe you are fully clothed - the time is now to look for holes aka places that need (software) patches - or maybe new engineering.

And, when it comes to AIX - time to activate core features - some around since the early 90's - and maybe start wearing armor as well.

- Syslog: check - using that (90%+ of the places I visit)
- Audit: we have it turned on (- does that count? 20%, 75% not even activated)
- IPSEC filters: No need - we have firewalls for that (98%)
- TE: (heard about that - does it hurt - 90%)
- EFS: (Oh, no, please no: 98%)
- RBAC: (We have looked at it - prefer sudo)
- SUDO: we have it installed, "sudo su -" is great (80%+)
- etc.

In short: TIME TO GET SERIOUS ABOUT SECURITY!