Who watches the watchers?

Analysis of insider threat based on a system administrator interview.

Antti Hämäläinen, 17.8.2016
ITKST45 coursework, University of Jyväskylä

The newspaper interview

- ”Die unheimlichen Götter” - Tages-Anzeiger 18.2.2014
- “I am God in this environment”
- One of 10 “system administrators” in a company of 20 000 employees
- He shows salary documents, personal files of a company manager, newest research results
- “I could stop the business for a month within 10 minutes”
- Risks: company data stolen, private data stolen, sabotage
- “1/3 of IT admins (2009 study) admit having snooped confidential data”

Comparison to Snowden (2013)

- The admin: ”if he’s caught looking at sensitive information, he says using “data error” as an excuse always works”
- Snowden: “As a systems administrator he was responsible for conducting routine network maintenance. That could include backing up the computer systems and moving information to local servers, investigators were told.”
- Particularly difficult to prove what is inappropriate “browsing” vs. “necessary spot checks”; mass data copying should be easier to detect

Why admins have such power?

- Best practices and formal standards exist (e.g. ISO 27001 etc.), but it's nearly impossible / expensive to prevent all risks; hard to justify the value of ”preventing a risk”
- One study on network security professionals: 31% have no security staff; ”network professionals” often perform more ”security” tasks than ”security” staff
- Regular or external users access to individual documents may be often audited, but system admins need ”full access” at some point
- Assessing ”unnecessary access” requires expertise

Other cases

- Bradley Manning 2010 (Wikileaks)
- Leaks by ”regular users” (sometimes caught based on audit trail)
- ”Photographing screenshots” is hard to prevent

Best practices against insider threat

- Risk assessment (what data is where, how could it leave the systems), ”acceptable risk”
- Separation of duties
- Enforce policies on accounts, backups, technical users
- Audit trail and monitoring (especially Internet connections), random audits?
- Monitoring suspicious behaviour
- Broad set of stakeholders in security programs
- Security awareness; transparency is also for admins benefit

Technical solutions

- Control removable and physical media
- Encrypt data (encrypt/hash database values; encrypt e-mail; encrypt documents in DMS infrastructure)
- Personal user IDs, audit trail
- Disaster recovery concepts (periodic backups, backup systems) to mitigate sabotage impact

- Technical solutions are only tools to support people based solutions!