Who watches the watchers?
Analysis of insider threat based on a system administrator interview.

Antti Hämäläinen
ITKST45 coursework
University of Jyväskylä, Finland
Version 6.8.2016
antti.p.hamalainen@jyu.fi

"I am God in this environment". This is how the newspaper Tages-Anzeiger begins the report (Schmid, 2014) interviewing an anonymous IT system administrator, who sits at home, with long hair and jeans, working over a remote connection with his laptop on the kitchen table. He spends half an hour showing his powers to the reporter. He is working in a corporation with 20 000 employees. He demonstrates his access to personal and company secrets and claims he could stop the business for a month within 10 minutes.

How realistic is this scenario and could this happen in all organizations? The article points out that there are ISO certifications and best practices available. But can insider threats be completely mitigated? In this essay I will look at the insider threat of organizations, in particular threats from IT staff, and ways to mitigate the related risks. I am focusing the discussion on administrators, who knowingly break the rules (as opposed to ignorance), and analyze the claims made in this interview.

The interview is "post-Snowden", published in February 2014. Naturally, the administrator's comments are to be taken with a grain of salt. It is possible he is trying to impress the reporter and cutting some corners. Nevertheless, the interview is logical and his claims realistic. The administrator shows salary documents, personal files of a company manager, newest research results. The information about company secrets or managers personal affairs could be valuable to sell competitors or use for blackmailing, but he claims he doesn't have the "criminal energy".

According to the administrator, there are 10 people like him in his company. All of them have access to the entire network of the firm, "without leaving suspicious trails". He claims that when moving data it's a necessity to open files anyways as random sample to check the results, and that if he's caught looking at sensitive information, he says using "data error" as an excuse always works.

Did organizations learn from the Snowden case?

The Edward Snowden case in 2013 raised information security awareness in the public eye (see Basani 2013), but the interview is a good example of the practical reality presumably in many IT companies. It's worth emphasizing that the NSA, one of the most advanced organizations in the world specialized in information security, was at least until 2013 sloppy in its internal controls in the way the Snowden case revealed, and that case happened three years after the Bradley Manning's widely publicized Wikileaks disclosures in 2010 were expected to have improved general security awareness. How much can we expect from regular companies to whom IT and particularly IT security are not the core business areas, but only play a secondary role supporting the business?

Edward Snowden was not a foreign spy or hacker attacking the systems from the outside, even though there have been from the beginning suggestions from American and European intelligence leaders that he may have been co-operating with a foreign government to begin with (see Sanger et al. 2014 and Elflein et al. 2016). Whether working on an assignment or with personal motives, he was an insider administrator in an organization specialized in information security affairs - and he was able to steal hundreds of thousands of documents, without being caught. This particular theft only became public because he handed over the documents publicly. How do we know how many similar security breaches have been carried out by foreign governments or competing companies in traditional industries?

Similarly as the administrator interviewed in the Tages-Anzeiger article, Snowden had been able to mislead investigators by providing a technical excuse: "In at least one instance when he was questioned, Mr. Snowden provided what were later described to investigators as legitimate-sounding explanations for his activities: 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." (Sanger et al, 2014). There apparently were some level of automatic controls and monitoring processes in place, but at the end of the day it seems the human factor failed in judging and reacting to the findings.

Why do the system administrators carry such powers?

In short, most solutions to insider threats are somewhat well known and do not require new technology or solutions. There are best practices and tools available – more on these later in this article. Security, however, comes at a cost and requires investing in the knowledge. Security measures may be considered as extra work, and typically many IT security measures – especially those related to insider risks – are an extra nuisance, and "preventing a risk" brings no tangible benefits in the short term. It may be difficult to justify spending extra time and effort in hardening servers, updating technical passwords or requiring complex processes for access management just to prevent something that may or may not happen in

the next 10 years, when a manager requires a quick installation, quick setup of access and quick business results. In a small organization it's possibly even a calculated, known decision based on necessity to just trust the 1-2 key IT administrators and take the risk.

Adnan et al (2014) conducted a comprehensive analysis of network security professionals daily tasks based on an online survey and previous research, and found out that bigger proportion of "network" professionals perform typical daily security-related activities, compared to "security" professionals. In their survey 31% of the respondents worked within organizations that do not have dedicated security staff. We can assume that generally especially organizations with small IT staff are less likely than bigger organizations to have the capacity to dedicate people to IT security, and IT security may typically be simply defined in the list of tasks IT administrators are responsible for.

One of the risks, naturally, is that "nobody watches the watchers". The IT administrator may be the only one to even be aware of all security related technical details. It would be good if the organization could separate the roles of IT security officers and IT administrators. The security officer should not have access everywhere, but could have access to security relevant log information, which the IT admin would not be able to manipulate. There is, however, a risk of the administrators being untouchable even when an IT security responsible has been named in the organization. The security professional may lack the deep technical knowledge required to accurately and comprehensively assess all security related risks or findings. Whether the security responsible is independently responsible for monitoring everyone or working in co-operation with the administrators, it may not be in the administrator's interests to proactively point out all possible vulnerabilities for a security review, if he wants to be able to get his daily work done without delay.

Transparency and proper security measures would, however, be also for the benefit of the IT administrator himself, not just for the organization. If there are no audit trails and logs of all activity, and someone (like an employee of the company in the news article) is being blackmailed with some personal information, or someone takes advantage of company secrets, and there are suspicions towards the IT administrator, how can he prove that he did not do it – especially if nobody else seems to have the access to such information? Legally a "doubt" can hardly bring someone a conviction, but it can make a company lose clients or an administrator lose his job, if they are unable to prove who leaked sensitive information and how.

Cases where regular policemen have improperly viewed celebrities' police records out of curiosity have been highly publicized in Finland (see Reinboth et al. 2014, Teivainen 2016), and people fined by the dozens for looking at 1 document of 1 celebrity through the normal user interface. But has anyone seen system administrators, who have access to bigger amounts of data, publicly caught for similar misuse?

Solutions and best practices to counter insider threat

The fourth edition of the Common Sense Guide to Mitigating Insider Threat (Silowash et al. 2012) presents 19 best practices, based on analysis of over 700 insider threat cases and ongoing university research. The practices include, grouped and simplified:

- considering insider threat in risk assessments, and knowing what type of data is processed and stored and where, and how data could leave the organization's systems
- enforcing policies and controls regarding passwords, account creation, changes and termination as well as backup and recovery
- using extra caution with system administrators and technical users, and enforcing separation of duties
- logging, monitoring and auditing employee actions, in particular regarding social media, any cloud services and all remote access
- monitoring suspicious behaviour and issues in work environment

Gelles et al. (2015) define ten high level practical considerations to mitigate insider threat, focusing more on the people and processes. These include:

- Defining the threats and acceptable risk
- Including a broad set of stakeholders to define the security program, organize customized security training for different groups, and constantly evolve the program
- Focusing on the people centric solutions, supported by technical tools
- Establish random auditing and detect suspicious behavior patterns

Assessing the sample case

How realistic are the scenarios mentioned in the article, and would the solutions help in the example case?

There are at least two or three separate risks mentioned in the article:

1. company data being stolen
2. private personal data being stolen
3. operational risk of sabotage – "stopping the business"

Many of the best practices mentioned are possibly in use in the sample organization. We don't know if the organization's risk assessments have identified the risks related to insider threat and the type of data stored – it's quite possible that the risks have been identified, but not prevented completely. An organization with 20 000 employees would probably have dedicated IT security professionals. The fact that the employee mentions having to resort to "excuses" to justify why he has viewed private data suggests that there are monitoring mechanisms and mitigation processes in place, although they seem to be not implemented properly or backed up with enough of technical expertise to correctly assess the data privacy violations.

We don't know if the organization has implemented measures to prevent data leaving the systems – possibly the administrator can view individual documents on his screen, but could not necessarily mass export the files to an external system. Viewing individual documents on screen could still be enough to steal data, and can be very hard to detect, as it doesn't differ from regularly viewing the data for legitimate purposes. For example in 2012 the German tax authorities informed they had bought data of over 1000 tax evading German clients with over 3 billion francs property from an anonymous Swiss bank employee, who had put the data together by photographing computer screen views, and as of 2013 the employee had not been identified (Rutishauer 2013).

What seems clear in the case, however, is that there are no technical restrictions to viewing data by system administrators,

regardless if the viewing is monitored or not. Based on the interview, it seems like the most, if not all, of the company's business secrets as well as employee's private information is stored in unencrypted formats in the infrastructure file system. This is presumably still quite typical, although there would be moderately easy ways to mitigate such risks. Employees could use encrypted e-mail for internal or personal communication and company documents could and should be stored in a proper document management system, which would make "browsing" for random interesting documents directly in the backend systems difficult. Applications could also keep an exact audit trail of who has viewed which customer's data and when. Using such measures, however, comes at a cost (extra effort and infrastructure). Keeping extensive logging information may not be cost efficient, either, and it may not be practically possible to extract the employee identifying information, especially if the employee is using a non-personal technical administration account in the maintenance (a practice against typical guidelines, but not uncommon).

Typical system administrators perhaps almost necessarily have some "powers" to bring down the systems, if needed – for example, ultimately someone needs to have access to the physical datacenter, and could physically destroy devices. Most likely they would, however, not be able to do so without being caught, and there are no publicly known "suicide hits" to a data center to date.

There are also backup systems (typically in separate physical locations) and periodic data backup policies, which typically would limit the damage – even if the employee manages to corrupt data or systems in a way which is replicated to backend systems. Therefore the notion of being able to shut the business in 10 minutes could be basically possible, but it's possible the impact would rather be around 2 or 5 days rather than a month, and it's difficult to think of a realistic situation and motive for such a sabotage with almost a guarantee of being caught. Perhaps in a realistic sabotage scenario the person would be paid by a competitor or a foreign government, would carry out the attack over remote access, and would be able to physically and permanently leave the country immediately, knowing that his destination would not turn him over.

Some of the organization's best practice policies which may not be very relevant for the particular security issues discussed in the interview are the policies related to backups, passwords and changes, monitoring behavior and remote access. The employee interviewed is using legitimate, active passwords, is accessing data remotely as part of his legitimate work, and presumably has not been caught acting suspiciously or having a criminal history which a background check would reveal.

Conclusion

This article has analyzed the sample case, which demonstrates the kind of insider risks that an organization may have from its IT employees. This article has listed some best practices to counter insider threat, and analyzed their applicability in the sample case. The scope of the risk is not thoroughly or critically assessed in the sample article. There is not enough information to determine whether the employee could in fact technically perform a mass theft of data or whether such data export is technically blocked, and neither it's possible to determine whether such actions would trigger actions in the monitoring systems or at the very least be trackable afterwards. It seems plausible that the employee's claims are valid, if perhaps exaggerated, and the situation seems somewhat typical to an IT organization's system administrator.

References

Adnan M, Just M, Baillie L, Kayacik H G (2015). Investigating the work practices of network security professionals. Information and Computer Security, 23(3), pp. 347-367.

Basani V (2013). Edward Snowden and the NSA: A Lesson About Insider Threats. Bloomberg News 3.7.2013. Available online: http://www.bloomberg.com/news/articles/2013-07-03/edward-snowden-and-the-nsa-a-lesson-about-insider-threats [referenced 3.8.2016]

Elflein C, Hufelschulte J, Spilcker A. Nach diesem Interview werden Sie nicht ruhiger schlafen. FOCUS issue 16, 16.4.2016. Available online: http://www.focus.de/politik/deutschland/sicherheit-terror-durch-dschihadisten-die-bedrohung-europas-ist-realitaet_id_5438633.html [referenced 22.7.2016].

Gelles MG, Mitchell K. Top 10 considerations for building an insider threat mitigation program. Journal of Threat Assessment and Management 2.3-4 (2015): 255.

Reinboth S, Teivainen A. Police officers snooped into death of Mika Myllylä out of curiosity. Helsinki Times 28.3.2014. Available online: http://www.helsinkitimes.fi/finland/finland-news/domestic/10013-police-officers-snooped-into-death-of-mika-myllylae-out-of-curiosity.html [referenced 3.8.2016].

Rutishauser A. "Der UBS droht schon wieder eine happige Busse". Tages-Anzeiger 30.10.2013. Available online: http://www.derbund.ch/wirtschaft/unternehmen-und-konjunktur/Der-UBS-droht-schon-wieder-eine-happige-Busse/story/10926838 [referenced 3.8.2016].

Sanger D, Schmitt E. Snowden Used Low-Cost Tool to Best N.S.A. The New York Times, 8.2.2014. Available online: http://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html?hp&_r=2 [referenced 3.8.2016].

Schmid, S. Die unheimlichen Götter. Tages-Anzeiger 18.2.2014. Available online: http://www.tagesanzeiger.ch/digital/daten/Die-unheimlichen-Goetter/story/11554542 [referenced 1.7.2016].

Silowash GJ, Cappelli DM, Moore AP, Trzeciak RF, Shimeall T, Flynn L. Common sense guide to mitigating insider threats, 4th edition. Published by CERT, Software Engineering Institute, Carnegie Mellon University, December 2012. Available online: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1669&context=sei [referenced 1.8.2016].

Teivainen A. Dozens of officials charged for snooping into notorious murder case. Helsinki Times 20.4.2016. Available online: http://www.helsinkitimes.fi/finland/finland-news/domestic/13940-dozens-of-officials-charged-for-snooping-into-notorious-murder-case.html [referenced 3.8.2016].