The White Knight - All's Well that Ends Well

Uwe Schmalfeld (uwe.schmalfeld@franken-online.de)

Scenario

The scenario is like plotted. Additional we assume that access to FileX is possible from the internet, protected by username and password, but no further authentication methods. Big uses this access from home and on travel.

Target

Primary target for our attack is Big. Big is responsible for the company as a whole. He sees single aspects like the IT as of great importance and may have some affinity to IT, but in order to save the company as a whole he will not hesitate to disobey internal policies, if it seems to be required. Secondary target is Sydney. As Sydney is a (mostly) female name we assume Sydney is a woman what might have some influence on details of the attack, but is not crucial. Sydney is a defender and could possibly discover and fend off the attack. So what we do is taking Sydney off the game. Other persons are not involved.

Basic idea

The attack consists of distraction, transfer of trust, DOS and phishing. What we do is to capture the inherent business related 'ribbon of trust' between the boss Big and his IT-expert Sydney using a kind of Man-in-the-Middle-Attack. This captured trust we use for a phishing attack on Big. In order to have enough time, the attack should take place at the beginning of holidays (i.e. Christmas). First we will bring Sydney offline in order to detain Big from contacting Sydney and asking for help. Then we bring Big into a pretended concerning situation about his company's financial affairs. We nudge Big to get access to the company's data, esp. FileX. We now disturb this access with a DOS-attack and appear as the white knight to rescue Big.

Actions

Phase 1: Gathering the required information (a couple of weeks before the attack)

We need the mobile numbers of Big and Sydney and some context-information about the relationship between them. Getting the phone numbers should be no problem as both people are in outstanding positions and we can easily pretend business related and urge needs for contacting them (i.e. confidential business resp. IT-emergency). In order to get more information about the relationship between these two we set up a fake anonymous telephone survey to Sydney with a subject like "Work-life-balance in IT-departments". Within this survey we ask together with some concealing questions, weather private or business-phones are used in IT-emergencies, weather the boss usually calls at home and vice versa and when it was the last time the boss expressed a reasonable compliment for good work. Of course we ask NOT for any 'confidential' information.

Phase 2: Cutting the line between Big and Sydney (evening of the last working day before holiday)

a) If Sydney is usually called on her private phone we post her phone number on a lot of porn-dating-sites, real estates- and automobile-trading platforms pretending to offer very good occasions. After a couple of hours this should lead to a lot of annoying phone calls so Sydney probably will switch off her phone. In case she typically will be called on a separate business phone instead we have to wait until late night. Then we run an old analog fax machine with a redialing function and feed it with her number. Now Sydney will probably not answer to calls from Big.
b) At late night Big receives a message (i.e. SMS) from "Fred", pretending being a friend of Sydney. The message says that Sydney is in medical treatment for now and needs absolute quietness at the moment. With respect to our 'survey' we can control the effect on Big so he should take it for serious but does not undertake further action: The closer their relationship is the more cautious the message should be. If Big nevertheless asks back Fred can foreshadow a suicide attempt with sleeping pills, but avoids mentioning it directly.

Phase 3: distracting Big (The following evening)

Next day in the evening Big gets a phone call from "Dr. Arnold", pretending to be an accountant of one of his company's customers. "Dr. Arnold" pretends to be investigating a strong suspicion of defalcation. The amount

missing is about 2 million € and the defrauder may also be among Big's financial employees. Arnold pretends that he wants to clarify his suspicion prior to involve the police. So he asks Big for cross-checking the overall order values in a personal telephone conference within a very short time (i.e. one hour). Big should ensure to have the latest figures ready, as they might have been manipulated a short time ago.

Phase 4: attack (a little later same evening)

Weather Big is believing Dr. Arnold's story or not, he will probably try to get access to his company's data as soon as possible. We prevent him from success with a DOS-attack either to Big's internet-equipment or to the company's Cloud. Sydney should now be "offline", either still bothered or we use again the fax-machine. In the following minutes "Fred" is calling Big. He tells in a harangue, that Sydney is already getting better, that she is now sleeping again but the doctor says this is ok, that she feels so sorry about what happened and everything is going to be alright. But Fred feels to be in a tight spot because Sydney does not want Mr. Big to know about what happened and he did not tell her, that he already has contacted Mr. Big. Fred explains he just has done this as he is also working as an IT-Admin and therefore he knows about the responsibility and that problems occur usually on holidays. At this point, Big will at least tell Fred, that he is trying to get access to his company's Data but cannot get through. This causes Fred to switch to "support-by-phone-mode". Now Big will trust the "IT-Expert" "Fred" and Fred guides him to a fake "workaround-routing" to bypass the "malfunctioning Service-provider". This is our own simple fishing-site, pretending to be a kind of workaround-backdoor to the cloud. Big will most probably type in his password.

Phase 5: cleanup

After some unsuccessful attempts Fred guides Big back again to the usual path and, as we suspended the DOS-attack meanwhile, Big should get access now. Fred, still on the phone, ends conversation asking "Mr. Big" not to mention anything to Sydney. After some time "Dr. Arnold" is calling. He apologizes for the disturbance and gives the all-clear. He states that in fact no money was missing; it has been just a tricky miscalculation in his own figures. If we have posted Sydney's phone number, we should now delete it as far as possible in order to avoid or cover the tracks.

Result

We now hold the appropriate credentials to access FileX. And what is even better: No one has noticed it. Big will probably not even remember that he has entered his password in a suspicious environment. Sydney may have recognized the DOS-attack and might think, she was personally attacked by some kind of personal revenge. But even if so, she will probably not find a correlation to the company and most probably none to Big. Big may think he knows a secret from Sydney but will probably not talk to her about that.

Countermeasures

This attack could not be prevented, but at least made insufficient if Big had to use a two-factor-authentication method (basing not only on knowledge, but also on possession).

Only Big could be able to detect and defend the attack. So an effective countermeasure could be to set up mandatory IT-security trainings for managers and take this scenario as a real life training-set. Usually IT-Security is treated as "something the IT has to deal with" and managers are not really involved in. Even in IT-Security seminars social engineering is often mentioned but not in detail and no countermeasures are trained. But if Big would be aware that he personally is one of the top targets and has an idea, how he could be hit, he probably acts in a different manner.

Possible Evaluation

The most crucial part of this attack seems to be the timing between the Initiation of the attack by “Dr. Arnold” and the appearance of “Fred” as the White Knight. It is necessary to estimate this timespan with the appropriate exactness and it is an interesting question, weather this is possible or not. An evaluation setup could be the extension of an already existing manager seminar and – in accordance with the organizer – perform the basic elements of the attack on some of the participants separately: DOS-attack on a phone number, transportation of trust and disobeying security policy.