UNIVERSITY, SCHOOL OR DEPARTMENT NAME

Investigation Case Study

Jordan Ell
V00660306

February 6, 2013

1 The compromised user account

Working as part of a presumed IT department at a company, this case study focuses on the exploits of employee Ulric Issac Darwin. Ulric has reported that his user id and subsequent email address at the company he works at has been hacked and broken into. This case study will focus on the ensuing example investigation that will take place follow the complaint of Ulric. This report is broken up into four subsections which outline the process involved in the investigation. First, initiation will outline the details of the investigation and set up any background knowledge necessary to begin the investigation. Second, coordination (done out of order for coherence of this report) will convey all coordination steps that should be taken in order to conduct the investigation. Next, documentation will outline what I did, what I found and my concluding recommendations. The documentation subsection will contain all the evidence found as part of the investigation.

1.1 Initiation

The issue at hand, is that Ulric Issac Darwin believes this user ID and subsequent email address has been compromised within the company he works for. This could have many different consequences based on the types of information he originally had access to with his account or what he was capable of. The obvious actor within this issue is Ulric himself. Some of the lesser known actors in this issue may involve Ulric's boss who will be primarily concerned with what is found out about this account. The IT department is also an actor as they are responsible for the security of information within the company

and could be having to deal with potential security leaks because of the account being compromised. Stakeholders of the company such as employees are also actors in this situation as their personal information or business information may now be compromised because of the account. Finally, every employee could be considered an actor as the compromise of the account could be an inside job within the company. Key assets of the investigation as previously stated are all the employee, company, or customer information is now potentially in jeopardy as the account may have access to this information. Also, the IT infrastructure in both technical and policy is an asset as these could either help or hinder the investigation and may have to be changed based on what is found.

For this investigation, two forms of resources will be used (although one of them is not actually preformed in this case study). For one, an interview will be conducted with Ulric in order to determine his story for how the account might have been compromised. Here, an attempt to establish a chronological nature of events will be made. Once this is done, Ulric's story will be broken down to check for inconsistencies or lies. This interview may lead to further interviews with other employees or stakeholders depending on Ulric's answers and demeanor. This interview is not actually conducted for this case study as Ulric is made up. The second resource used for this investigation will be technical logs stored and monitored by the company. These logs include Active Directory authentication, Outlook web access, and PIXIE logs.

1.2 Coordination

For the investigation team, I would use a team of IT team members from inside the company as well as an HR representative. The IT team members are there to check technical log and check for any technical irregularities that may arise during the investigation. These team members are key as they will have the expertise to find quantitative evidence to support any claims that the investigation team may find. The HR representative is there to be apart of the interview of Ulric and any interviews that may emanate from that. The HR employee has made a career of dealing with people and should become a great assistance in any interrogations that may occur.

In terms of notification and stakeholder information, the most obvious person who comes to mind is Ulric himself. He should be kept notified of any findings in the investigation as they may cause positive or negative repercussions for his future career. Ulric's boss as well as any superior employees whose reputation, job, or own employees should also be notified to the investigations findings. Ulric's boss may have to take immediate action against individuals from the findings. Messages may need to be relayed to the rest of the employees at the company to avoid future complications that may be found.

1.3 Documentation

I would outline this section in the following ways: what I did, what I found, and future recommendations for Ulric and the company. For the purposes of this case study, I did

not interview Ulric, however, given a real investigation, this would have occurred as well as any follow up interviews of company employees that might have been necessary. What I did do however, is parse through all the given email and Outlook logs that were given for this case study. These logs were able to provide all the email send and received got eh account in question as well as remote access to the account from outside the company network.

What I found was that Ulric was using his email account for personal use to email and receive emails from outside the company addresses including personal contacts as well as personal information such as email notifications from restaurants and other services. I have also found that Ulric's email account was accessed from outside the company at times where Ulric is known to be at work. These accesses were all from the same machine and what is believed to be his wife's laptop. Therefore, I believe one of two things has occurred. Either one, Ulric's wife has unauthorized access to his email account, or two, the email account is shared between the two. If she has unauthorized access, it seems as though she has found him in a personal relationship outside of his marriage with the owner of the email address ladybird1@yahoo.net. If the email address is shared it seems as though Ulric is lieing to us to avoid being caught in his extra marital affair.

Where either of these stories are true, I have a few recommendations to make for the company. Number one is that a work email address should never be used for personal or non work related items such as chain mail, emailing non employees or non customers, or personal financing etc. Two, email accounts should never be shared with anyone outside or even inside the company. The risk of outside party members is obvious with non authorized access to company data, while not sharing with internal company members is to retain accountability between members of the company and who is taking which actions when investigations are being done. Finally, the company should have a better authentication process in place for remote access of these accounts. This may be done by only authorizing certain machines into the network or notifying personnel when their account is being used for the first time by an unauthorized machine.

1.3.1 Evidence

The evidence for the claims listed above can all be found inside the logs provided to the investigation team. From the Outlook Web Access logs, we know that Ulric's account is being accessed by a third party from outside the network at ip address 76.193.130.252. These accesses are also at times when Ulric is known to be at work, thus it must be a third party. We can also see from email header provided that this IP address matches the user using the account unknsub@shaw.com from who Ulric has frequent emails with. Next, we can see that Ulric has emailed ladybird1@yahoo.net with the subject line Happy Tuesday Baby, which we can assume is not pleasent news to his wife who is actually the owner of unknsub@shaw.com. From these pieces of evidence we were able to draw up the two scenarios presented above. Either Ulric's wife has unauthorized access to his email and has caught him in a relationship outside his marriage (in which case his email

has technically been hacked) or two, Ulric has shared his email with his wife, which is far more likely given her frequent activities on his account, and is now lieing to try and presumably protect himself from his wife (in which case he has not been hacked).