Sjoerd Halmans

Research

This document will go into detail on the research I have done on the subject of social engineering, and how a user of Productio can protect themselves against it.

Social engineering within productio

And how to protect yourself against it

Inhoud

[Preface 2](#_Toc74901763)

[Threats 3](#_Toc74901764)

[Scenario 1 – the loose thumb drive 3](#_Toc74901765)

[Scenario 2 – The wrong credential call 4](#_Toc74901766)

[Scenario 3 – Sorry, gone phishing! 4](#_Toc74901767)

[Minimizing Threats 5](#_Toc74901768)

[Scenario 1 – Protect your ports 5](#_Toc74901769)

[Scenario 2 – Identify before you comply 5](#_Toc74901770)

[Scenario 3 – Leave out the links 5](#_Toc74901771)

[Conclusion 6](#_Toc74901772)

[References 7](#_Toc74901773)

# Preface

While a large part of securing an application lies with the actual techniques used while programming it, a large threat looms around the corner waiting for anyone that has forgotten about it.

Social engineering is the art of hacking a system/company with little use of a computer, and while you may secure an application against all of the OWASP top ten threats and maybe even more, one human mistake can still allow your application to be breached.

This document will explain how users of Productio can protect themselves from falling prey to this, and what protocols should be in place for certain users.

Much (if not all) of the knowledge used in this research has come from reading Kevin Mitnick’s book on Social engineering ‘the art of deception’ and following a social engineering course at Fontys. Kevin Mitnick himself is a retired social engineer/hacker himself, now working as a security consultant, thus a lot of the stories and methods described in his book are from experience.

“The human factor is truly security’s weakest link”

Mitnick, K (2003). *The Art of Deception: Controlling the Human Element of Security*.

# Threats

To come up with ways to protect ourselves, we should first clear up what the actual threats are. To do this I will name a few scenarios in this chapter and explain how to protect ourselves from it in the next chapter.

## Scenario 1 – the loose thumb drive

Let’s say Productio is being run locally by a company (from now on referred to as company X) on their intranet, but allows people working from home to access it by only port forwarding the gateway and frontend.

Doing this allows people working from home to access the application, but also disallows any would be attackers from accessing the API’s and databases directly, as they are simply not reachable without going through the gateway. (which is protected by Auth0)

Now let’s say our attacker were to somehow make his way into company X posing as an employee or maintenance personnel for instance. If they were to then plug a thumb drive with malicious software into a machine connected to the same network as the API’s, they could create a backdoor that would allow them access outside of the network.

A seemingly innocent way for attackers to enter a building that requires key card access is the heavy object trick. Let’s say for instance that our attacker needs to get through a door that requires a key card to open, they will bring with them a seemingly heavy or bulky object, and simply wait at the door.

Later, a random employee arrives at work and needs to get through the door as well. Spotting our attacker with the heavy object, they open the door for them without thinking about possible security threats.

“It’s human nature to trust our fellow man, especially when the request meets the test of being reasonable. Social engineers use this knowledge to exploit their victims and to achieve their goals”

Mitnick, K (2003). *The Art of Deception: Controlling the Human Element of Security*.

This same threat can happen without the attacker even entering the building. Say for instance you are parking your car in the company parking lot, and spot a thumb drive on the ground, curiosity would tell you to grab it and plug it into your work computer to check it out. Sadly, this just infected the entire company intranet with malware and a back door.

## Scenario 2 – The wrong credential call

Productio allows internal HR employees to manage the credentials any user has within the application, and with this power comes great responsibility.

As Kevin Mitnick explains in the previously mentioned book, Just asking for something can be the most effective way to break into a system, let’s say we have a HR worker that is responsible for giving out credentials, and our intruder has made an account with no permissions and only the ability to log in but nothing else.

The attacker would make a phone call to the HR employee, and claim to be someone they are not, talking their way through the conversation and staying friendly, the employee may be manipulated in following their request of giving the account permissions they are not allowed to have, this is one of the most basic ways of using social engineering but also one of the most dangerous when we take human nature into consideration.

## Scenario 3 – Sorry, gone phishing!

Phishing can be a threat in many ways, but in this scenario we will talk about how it could tie in with one of the OWASP top ten risks, Broken authentication.

One of the most common and most dangerous threats on the internet is phishing mails, and while they can come in many forms, the personal ones are the ones that are the most dangerous most of the time.

Let’s say that our attackers has gotten his hands on the email addresses of our employees, this allows him to send phishing mails to all of the users of our system, something they could do is send a mail about a companywide Christmas celebration and ask employees to click a link to confirm that they will be attending.

To make the email even more believable, an attacker could research company X on for instance LinkedIn, and find out the names of certain higherups that would be sending these kind of internal emails. Clicking on a link in one of these emails can harm your computer and Productio in many ways, if you allowed the attacker to download something onto your computer it could already be compromised with a trojan horse, or if the link lead to a fake website that asks for your credentials you could have given them your account. Luckily, Productio guards it users against some of these threats, an attacker will have to get past the multifactor authentication to log into another person’s account.

Sadly there is still the risk of session hijacking, if you were to press an attacker’s link while stilled logged into Productio, they could hijack your session by stealing the login cookie in your browser and pasting it into their own, effectively logging them into Productio with your account.

# Minimizing Threats

In this chapter we will look at the scenarios we have discussed in the previous chapter, and see if we can find a way to minimize the threat that these scenarios pose.

## Scenario 1 – Protect your ports

In the first scenario we talked about physical access to machines and how it can risk a security breach for Productio. A fool proof way of negating this risk is very simple, Port locks! Port locks are little USB devices that you can stick in your USB ports and lock with a kind of key, this allows you to lock any vulnerable USB ports that an attacker could use.

Another way is to have a clear protocol on letting people into the building, if you do not recognize someone, make sure to ask them for an ID badge or get them to show you their key card, it might be a little less altruistic, but it will protect the company.

Finally there should be a rule on plugging unknown devices into the company network machines, informing all your employees about these risks and disallowing the use of unknown devices will greatly diminish the risk of this scenario happening and breaching the data you’re storing in Productio.

## Scenario 2 – Identify before you comply

In the second scenario we talked about the risk of a HR employee giving away permissions due to being sweet talked by an attacker, a quick and easy way to mitigate this risk is by setting up a protocol that these employees need to follow (and have the appropriate trainings to enforce the use of said protocol). An example of this is asking the caller for information that only the person itself and HR employees would have access to.

If all else fails, Productio could be configured to only allow certain individuals to manage certain permissions, and enforce that all changes be done in person instead of over the phone.

## Scenario 3 – Leave out the links

In our third and final scenario, we talked about how phishing can expose Productio and Company X’s network. A good way to minimize the risk of phishing happening is by make sure that all emails that come from addresses other than your internal company mail has any and all links removed/censored.

Doing this allows you to give users a warning that this mail is from someone outside of the company and that any link they press might be dangerous and should only be pressed if it is from a trusted source.

# Conclusion

This has been a short document on how to protect your company running Productio from the most common social engineering attempts, I would like to take this moment to suggest “The art of deception” written by Kevin Mitnick to anyone reading the report. It is a great book and goes into way deeper detail on how social engineers go to work and what threats are out there, way more in depth and precise than I will be able to go in this research document.

I would like to thank anyone that read this report, and hope that it gave you new insights on security.

# References

Mitnick, K. D. (2003). *The art of deception: controlling the human element of security*. Wiley.