FASTPASSCORP

Spear Phishing News

IT departments are the target!

Introduction

IT security is high on the agenda for all serious enterprises. Investments in Hardware and Software protection, and Monitoring grows year after year.

But the most important element in data breaches is documented to be Social Engineering, and we don't see investments, or much action done to mitigate this threat.

To get access to the most critical IT resources the hackers now increase their attacks on the central IT-departments to get passwords and other assets to complete their criminal attacks. The criminal actors have learned that standard Phishing doesn't give results with professional IT-staff, so the method now is spear phishing (or vishing (Voice phishing)).

In this Newsletter, you'll see a curation of articles and blogs with research and statistics about this form of Social Engineering and published news related to real companies being breached by it!

We hope that this will motivate IT and Security management to initiate actions to improve protection against social engineering targeting the IT department (in particular the IT-service-desk) and other central staff functions.

Please forward material or inspiration you consider of relevance for this newsletter to fj@fastpasscorp.com

Regards,

Finn Jensen, Founder FastPassCorp

Password Security News

FASTPASSCORP

CHAPTER 1

69% of IT Departments have been Targeted by Vishing Attacks

We combined external research and statistical sources with data from our customers to answer a question closely linked to data breaches: Are IT departments victims of social engineering attacks? Our experience is that the idea of social engineering is well understood by IT-management, but the risk that their own department might be the victims are not generally accepted.

Specifically, we looked at the importance of the human factor and phone based social engineering (vishing) as part of data breaches. The importance of credentials /passwords in social engineering is included too.

In this blog we share the surprising results and add some suggestions for remedies!

Here is a Summary of the Key Numbers

1. **69%** of IT departments have been targeted by a vishing attack (Statista)
2. Vishing attacks have grown **550% in 12 months** (Agari & Phislabs)
3. **78%** of IT Service Desk managers fear a criminal can get a password from their supporters (SDI)
4. The human factor contributes in **82%** of data breaches (Verizon DBIR)
5. **25%** of Business Email Compromises (BEC) used a stolen password (Verizon DBIR)
6. **71.6%** shutdown rate on vishing calls after a 4 years' improvement program (Social-Engineer,LLC)
7. **64%** of users can't remember answers to their personal verification questions (FastPassCorp)
8. Criminals use passwords for data breaches in **50%** of incidents (Verizon DBIR)
9. **75%** hacker success when combining vishing and phishing! (Group-IB)

Everyone know that our IT-systems are targeted by criminals for financial gains or state purposes, and even government departments and agencies fall victim to vishing attacks. All competent IT-departments invest heavily in people, technology and processes to protect against attacks. New statistics from various sources as presented here, challenge if more attention and investments should be directed to the human risk factor!

The Human Element is a Factor in 82% of all Breaches

What about the human factor? If an employee unknowingly gives away critical information about the IT-system, then this is the key criminals need to open the safe. The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes, is called: Social Engineering in contrast to technical engineering, which is where most security investments are placed.

How much does social engineering scams count for when it comes to data breaches? According to ***Verizon's Data Breach Investigation Report 2022:***

The **human element continues to be a factor in 82% of all breaches.** (DBIR 2022 p 33).

It's important to understand that a data breach almost always requires many elements to be in place for the hacker to make a success. The human factor is just one element of the attack, but still without it, the attack can't be done. A stronger focus on preventing the human element to help hackers will obviously make a huge difference.

25% of BECs involve use of a stolen password – not phishing!

We might think that stolen passwords are the result of phishing attacks, where the criminal then use the password for his attack. But the hackers have other ways to obtain passwords.

Verizon DBIR 2022: Only 41% of Business Email Compromises (BEC) involved Phishing. Of the remaining 59%, 43% (in total = 25%) involved use of stolen credentials against the victim organizations.

Credentials means passwords in almost 100% of the situations! The question is: "How has a fraudulent operator **stolen the passwords for the 25% of the BECs?**"

The main methods for social engineering are:

Phishing: using e-mails to get individuals to reveal personal information such as passwords and credit card details.

Vishing: making phone calls or leaving voice mails to induce individuals to reveal personal or company information.

Smishing: an attacker uses a compelling text message to trick targeted recipients into clicking a link and sending the attacker private information.

For the criminals, Phishing and Smishing have the positive characteristic that it is very easy to automate and distribute to millions of users with a very low cost per transaction. This means that you only need a very low positive rate to be successful.

69% of IT-departments Targeted by Vishing Attacks

If you want to hack an IT-system, then the IT-people are the obvious group. They know (or should know) about phishing and are not easy targets for phishing and smishing campaigns. This might explain the strong growth in vishing attacks against IT-departments!

According to Statista **69% of IT departments have been targeted by Vishing attacks in 2021** which is an increase of 54% from 2020 based on 600 interviews.

Does this make business sense – for the hackers? Absolutely! If a hacker is successful in gaining the relevant data from the IT-department, they have the keys to the castle! A hacker only needs to succeed once to make it very profitable.

We think that the 69% who have reported the incident have avoided to be victims. The real victims who have disclosed important information including passwords probably don't know what happened! We can safely conclude that much more than 2/3 of IT departments have been attacked. We don't have the numbers for the success rate.

550% Vishing Growth

Is vishing only focused on IT-departments? No, it is much more widespread! A well-known social engineering methods is to call a user and pretend you come from IT-support, and need the user's password to solve an important technical issue. Other scams include phoning the finance department and impersonate the CEO to get a fast money transfer.

According to the latest Quarterly Threat Trends & Intelligence Report from Agari and PhishLabs **vishing has grown 550% from quarter 1 2021 to quarter 1 2022!**

> *"By the end of the year, more than one in four of every reported response-based threat was a vishing attack, and this may continue through Q1 2022."*
> *https://www.fastpasscorp.com/blog/vishing-cases-increased/*

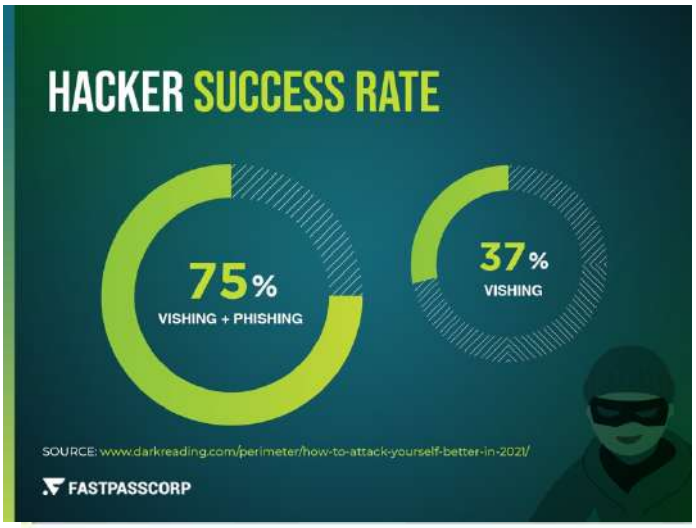
The growth is of a magnitude where much more attention is required from IT-security organizations to come forward with recommendations to protect against vishing attacks.

The IT-staff is generally very important for hackers as they have access to critical It-infrastructure. Obtaining their credentials is much more valuable than getting a password for an ordinary user.

75% Hacker Success when Combining Vishing and Phishing!

What can a competent hacker expect to achieve with a vishing campaign against a specific target? Is it at all realistic that social engineering with phones will get the desired results?

To assess the scope of the problem, Group-IB carried out a social engineering penetration testing project:



"Of the more than 100 social engineering testing projects we conducted in 2020, we discovered that voice calls ("vishing") were more effective than phishing emails with links to fake resources or executable attachments. Vishing, which had a success rate of 37%, is particularly effective because victims do not usually expect these calls"…." ***Vishing combined with phishing*** *(with both a link to a fake resource and an executable attachment) delivered* **ultimate efficiency: 75%** *of our social engineering testing attacks were successful in 2020.*

Source: https://www.darkreading.com/perimeter/how-to-attack-yourself-better-in-2021/a/d-id/1340686?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple

Do we really understand what this 75-percentage means? To me it means that a criminal can get information about critical infrastructure, other employees, and their passwords at a very low cost – and no real risk at this stage. Data breaches is a business now, and the hackers' efforts are directed where the best price/performance can be achieved. This success rate of 37% or 75% explains the 550% growth of vishing.

50% of Data Breaches can be Attributed to Leaked Credentials

What are the social engineers hoping to get from their activity? Passwords!

Alex Weinert (Director of Identity Security at Microsoft) states: "Remember that all your attacker cares about is stealing passwords...That's a key difference between hypothetical and practical security."

The very first summary illustration in the Verizon 2022 DBIR: stated **50% of data breaches can be attributed to leaked credentials (passwords).**

This confirms numerous other studies proving that the hackers need passwords as one piece of their puzzle. Password Policies to prevent that users make easy-to-guess passwords are extremely important. But if the hackers use social engineering, then they get even the complex passwords! Protection of passwords must include protective actions against social engineering.

Summary of Findings

Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities, and Botnets. All four are pervasive in all areas of the DBIR, and no organization is safe without a plan to handle each of them.

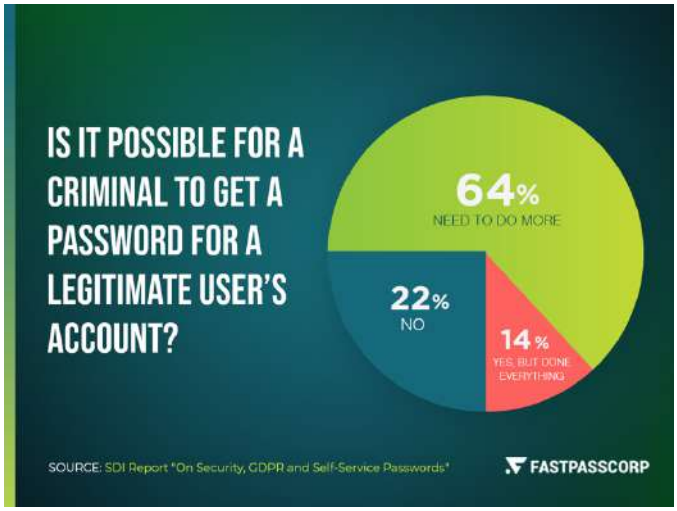
78% of IT Service Desk Managers Fear a Password Breach

A few years back Service Desk Institute (SDI) conducted a survey amongst their members funded by us. 78% of the managers feared that a criminal can persuade their staff to give away a password.

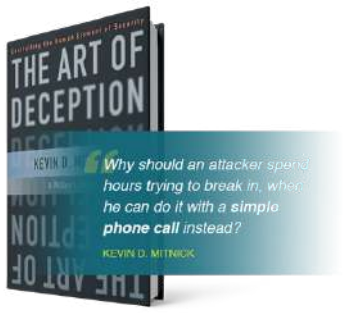
The question: “In spite of your authentication process, do you think it is possible for a criminal (internal or external) to get a password for a legitimate user’s account?

Of those who answered with YES or NO, a surprising 78% say YES. Only 22% are confident that their staff has strong enough procedures and training not to be victims of social engineering

Indeed, 14% had done all they can but realize that the risk remains. This is probably how it is when humans with emotions control a process!



See: SDI Report “On Security, GDPR and Self-Service Passwords”



It’s worth remembering what the well-known white-hat ethical hacker Kevin Mitnick writes in his book “The art of deception”: “Why should an attacker spend hours trying to break in, when he instead can do it with a simple phone call?”

71.6% shutdown rate on vishing calls after a 4 years' improvement program

The most recommended mitigation against vishing is training of the employees. The IT security consulting group Social-Engineer,LLC has published a case study from one of their assignments at a customer of app 18,000 employees.

Initially tests found a compromise rate of 46% and a 36% shutdown rate. After 4 years' engagement dramatic improvements were observed: 28.3% compromise rate and 71.6% shutdown rate. https://www.social-engineer.com/wp-content/uploads/2021/06/A-Case-Study-in-Vishing.pdf

The case illustrates that awareness and training can achieve significant improvements. But it also tells us that a hacker dedicated to the task with persistence can get results. It is extremely difficult to predict and control human interactions.

36% of Users can't Verify themselves with Answers to Challenge Questions

If a user has access to his corporate network, and you need to verify him on the phone, you can send him an email and ask him to read out the text or number you send. But if he has forgotten the password or claims he has (as in a forgotten password situation) and too is without access to his corporate email, how can the user then verify his identity?

If you ask a supporter in the service desk how often a special method of verification is successful, we have the risk, that the supporter in sympathy for the user "helps" a bit, simply because the supporter wants to help.

We have found objective facts from customers' experience with self-service of password solutions, where everything is logged in the verification process. We have analyzed more than 32,000 self-service transactions from our customers, to see what the user herself can contribute with in the verification steps. The FastPass self-service solution for password reset in most installations allow the user to select between multiple verification methods – in many cases they must use 2 factors to reset the password.

In the logs we can see if a user tries using a method and then fails. They might then try another test or call the service desk.

We can see that users in 36% of the cases can't remember the correct answers to their challenge questions.

The use of TOTP tokens has however a success rate of 95%. In most cases the tokens reside on the user's smart phone. Using a TOTP or a Push based app can be an excellent proof of verification.

It happens however that the user's phone is lost or forgotten, and you still want them back in work or assist them with important data for their task. Then you have to find other ways to verify them on the phone.

A social engineer will either spoof a phone number or claim it is forgotten, when he calls for passwords or information. So, you must be able to distinguish between the legitimate user and the false user.

Combining dynamic and contextual data from the system not available to any hacker will add a layer of security, which means that we reliable can verify the real users and discard the false. When in doubt call a trusted colleague to verify the person.

Some Real-Life Vishing Attacks on IT-departments

From the above cited statistics, it is obvious that some risk for vishing attacks against IT-departments exist, but do we know of real-life breaches? We have some prominent examples of this:

Twitter: Lessons learned from the Twitter Hack of 2020

Robinhood Data Breach: Robinhood Data Breach **and**

CISCO: CISCO Corporate Networked Breached

...but we believe it to be much more widespread. When a stolen password is part of an attack it is very difficult to research how the hacker has stolen it. The hack might even go unnoticed in some cases, where the criminal “only” steals a few million dollars and then vanishes without a trace.

In BBC News Security Analyst Joe Tidy wrote on the CISCO breach (Sept 2022):

The saying goes in cyber-security that “humans are the weakest link”, and once again this hack shows that it was an employee being fooled that let the criminals in.

Although the saying is true, it’s also extremely unkind.

The fuller picture emerging here shows that this hacker was highly skilled and highly motivated.

As we saw with recent breaches of ***Okta, Microsoft and Twitter***, young hackers with plenty of time on their hands and a devil-may-care attitude can persuade even the most careful employees into making cyber-security mistakes.

This form of hacking through social engineering is even older than computers themselves - just ask infamous former hacker Kevin Mitnick, who was sweet-talking his way around telephone networks back in the 70s. https://www.bbc.com/news/technology-62925047

We note that the list only includes IT-companies and Internet based business. It is unlikely that these are the only verticals to be attacked. It might however be so, that they are open and disclose their findings. Considering the facts in this blog there must be many more organizations

who have been victims of vishing attacks. They might prefer to keep quiet about it, or they might not even know it has happened!!

This form of hacking through social engineering is even older than computers themselves - just ask infamous former hacker Kevin Mitnick, who was sweet-talking his way around telephone networks back in the 70s. https://www.bbc.com/news/technology-62925047

We note that the list only includes IT-companies and Internet based business. It is unlikely that these are the only verticals to be attacked. It might however be so, that they are open and disclose their findings. Considering the facts in this blog there must be many more organizations who have been victims of vishing attacks. They might prefer to keep quiet about it, or they might not even know it has happened!!

Summary

1. Criminals use passwords for data breaches in **50% of incidents** *(Verizon DBIR)*
2. The human factor contributes in **82% of data breaches** *(Verizon DBIR)*
3. **25% of Business Email Compromises (BEC)** used a stolen password *(Verizon DBIR)*
4. Vishing attacks have grown **550% in 12 months** *(Agari & Phislabs)*
5. **69% of IT departments** have been targeted by a vishing attack *(Statista)*
6. **71.6% shutdown rate on vishing calls** after a 4 years' improvement program *(Social-Engineer,LLC)*
7. **36% of users** can't remember answers to their personal verification questions *(FastPassCorp)*
8. **78% of IT Service Desk managers** fear a criminal can get a password from their supporters
9. **75% hacker success** when combining vishing and phishing!
10. Many well-known companies have been hit by vishing attacks against the IT-department.

Conclusion

What can we learn from the above facts?

In general terms then vishing is growing very fast because it works, and is very difficult to prevent, as social engineering is about human behavior and emotions.

The IT-department itself, who has the responsibility for IT-security, is a target too because they have the most valuable assets = the credentials!

Passwords are a necessary piece in the puzzle for the hackers, and they can get the passwords from the IT end-user service centers through phone-based social engineering = vishing.

- **Criminals phone the IT-departments for passwords because it gives them the necessary results at the lowest cost.**
- **User verification must include IT-workflow with multiple verifications**
- **IT-service desks are not prepared for vishing attacks**

IT management can decide to do something about it now and protect their assets before the hackers start calling in. Or wait and be surprised when it happens.

Remedy: Awareness and Intelligent Workflow

What is the remedy against vishing attacks? We see a need for a combination of human involvement and forced IT-workflow:

1. Everyone in an organization can be the target of a vishing call. Education, training, information, and controls are necessary elements in preparing the organization against vishing (as well as phishing) attacks. Experience shows that it helps – but as it still continues and grows then the hackers find it efficient!
2. Where you have resources within your organization that have access to critical data and are expected to assist colleagues, you must implement a forced IT-workflow. If you just rely on “common sense” the hackers will ultimately find a way to succeed! Having a forced IT-workflow in place will take emotions out of verification, and it will prevent any data breach at the service desk and will ensure the hacker goes elsewhere.

Within the IT-service desk environment, the service desk supporters are there to assist users reset passwords. Even if they have a good written procedure today, a good social engineer can persuade the supporter to bypass the process in many ways “just for me today”! The **intelligent IT workflow** will instead verify the identity of the user based upon contextual and dynamic data and decide whether to provide a password or not. The consequence is that it is not necessary for the service desk analyst to have access to the administrative password reset tool – only the workflow has these privileged rights. The same process should be used in all situations where data or important resources are made available to users.

CHAPTER 2

Prestigious accounts being victims of Vishing attacks against the IT-department!

See real life examples of IT-departments hacked by vishing attacks.
Thanks to the transparency of these great companies, we know how the hackers did. Most companies breached don't want to display their weaknesses and keep quiet about the breaches. We can assume that it is a high number.

Twitter

The **Twitter hack of 15th of July 2020** proofs that Hackers go targeted for service desk employees.

The key phrases here are:

- **Small number of employees**
- **Phone spear phishing**
- **Mislead certain employees**
- **Exploit human vulnerabilities**
  - **Obtaining employee credentials**
  - **Specific employees with access to account support tools**

MailChimp

Mailchimp News 2023:
On January 11, the Mailchimp Security team identified an unauthorized actor accessing one of our tools used by Mailchimp customer-facing teams for customer support and account administration. The unauthorized actor conducted a social engineering attack on Mailchimp employees and contractors and obtained access to select Mailchimp accounts using employee credentials compromised in that attack.

Jumpcloud

The Identity Management company JumpCloud was hit by a spear-phishing attack orchestrated by a state actor! According to JumpCloud themselves: "*On June 27 at 15:13 UTC we discovered anomalous activity on an internal orchestration system which we traced back to a* ***sophisticated spear-phishing campaign*** *perpetrated by the threat actor on June 22*." https://jumpcloud.com/blog/security-update-incident-details

With the credentials obtained by the campaign the state actor injected data into the commands' framework: *"Continued analysis uncovered the attack vector: data injection into our commands' framework. The analysis also confirmed suspicions that the attack was extremely targeted and limited to specific customers."*

This case confirms the importance of protection against spear-phishing where attackers (simple, commercial and state criminals) target specific employees to get the necessary access to do data injection and other hacking activities.

CISCO

Network equipment manufacturer giant Cisco, confirmed on 11 August 2022, that their corporate network was breached by the Yanluowang ransomware group and they were able to obtain access to Cisco's employees' accounts. The attacker bypassed Multi-Factor Authentication (MFA) using a variety of techniques, which includes **vishing (voice phishing)** and MFA fatigue.
See the full story: https://beaglesecurity.com/blog/article/cisco-attack-by-yanluowang-ransomware-gang.html

LastPass

From HackerNews:

"The August 2022 incident, which remains a subject of an ongoing investigation, involved the miscreants accessing source code and proprietary technical information from its development environment via a single compromised employee account."

The unanswered question then is:

How did the hacker compromise a single employee account?

- **A criminal employee?**
- **An encrypted password captured in flight?**
- **A successful phishing attack against an IT employee?**
- **A password issued from the help desk to a hacker?**

The easiest and cheapest method for the hacker is the help desk!

Verification of employees by help desks before they issue a new credential or password is a very weak link in most security protections.

Twilio

In the June 2022 incident, a Twilio employee was socially engineered through voice phishing (or "vishing") to provide their credentials, and the malicious actor was able to access customer contact information for a limited number of customers," Twilio said.

Robinhood

In November 2021 Robinhood was attacked.
In a post *to its blog, Robinhood says that the unauthorized party "socially engineered a customer support employee by phone and obtained access to certain customer support systems."*

This is a person-to-person skill obtained by criminals. They convince the service desk supporter to issue a password. Perhaps they are very good, perhaps the supporter is too busy. Perhaps his instructions are un-clear, perhaps he is not complying with them.

Reddit

Hackers have gained access to internal Reddit systems. They targeted Reddit employees with a sophisticated phishing campaign. They obtained an employee's credentials, and then had access to internal systems and documents. https://www.reddit.com/r/reddit/comments/10y427y/we_had_a_security_incident_heres_what_we_know/?mc_cid=37f39ce1ae&mc_eid=ac7ec55e98

Credit to Reddit for being open and transparent about the attack. This is in line with many other high-tech companies who have been victims in the same way like Twitter, Mailchimp, LastPass, CISCO….

The important lesson is that hackers use social engineering methods to convince employees to give away credentials like passwords and 2FA keys. Some hackers target the individual, others target the central service desks and pretend to be a real user.

Mitigation requires awareness campaigns for the general staff and secure workflow for identity verification for the central services: https://www.fastpasscorp.com/solutions/identity-verification-manager/

BBC Says

In BBC News Security Analyst Joe Tidy wrote on the CISCO breach (Sept 2022):
The saying goes in cyber-security that "humans are the weakest link", and once again this hack shows that it was an employee being fooled that let the criminals in.
Although the saying is true, it's also extremely unkind.
The fuller picture emerging here shows that this hacker was highly skilled and highly motivated.

*As we saw with recent breaches of **Okta, Microsoft and Twitter**, young hackers with plenty of time on their hands and a devil-may-care attitude can persuade even the most careful employees into making cyber-security mistakes.*

This form of hacking through social engineering is even older than computers themselves - just ask infamous former hacker Kevin Mitnick, who was sweet-talking his way around telephone networks back in the 70s. https://www.bbc.com/news/technology-62925047

CHAPTER 3

MFA Fatigue: Passwords are still important

Have you heard of "**MFA Fatigue**"? Neither had I! You might however have seen that Uber, Cisco, Microsoft have had data breaches recently– all including MFA Fatigue, so it is time to consider the consequences.

MFA Fatigue exploits **Multi-Factor Authentication (MFA)** solutions that send users sign-in approval notifications after account access attempts – as well as the fact humans get frustrated by endless streams of messages. In an MFA Fatigue Attack, the hacker will make multiple attempts to log into a given user account configured with multi-factor authentication, using stolen credentials, sending an endless stream of sign-in approval requests to the user's device. The intention is that the victim finally approves the request out of pure frustration or is convinced they've been asked to do so by their tech team.

Now, breaching a push-based authentication method should not open the doors to your systems as you still will have the user's password to protect you! This is the point of MFA or 2FA: The hackers must succeed in breaking two authentications. But if you have reduced your attention to password policies and processes because "we have MFA and then passwords are not that important!", then you are down to one-factor-authentication in reality. MFA Fatigue illustrates what has been said repeatedly by security experts: No authentication method is 100% secure!!

My advice is that your company makes a Password Protection Plan covering policies, processes, technologies, and organization. Passwords – as the “thing only I know!” must still be an important part of your protection!

Sources: https://www.fastpasscorp.com/password-protection-plan-download/

https://tech.co/news/mfa-fatigue-hackers

CHAPTER 4

50% of Data Breaches can be Attributed to Leaked Credentials

Hacking an IT-system is often like a puzzle and the hacker needs all the pieces to be successful. In 50% of data breaches, a password is required says Verizon DBIR 2022.

If we can prevent the hackers from obtaining important passwords, we will potentially have reduced data breaches by 50%, so we need to understand how hackers obtain passwords. This blog focuses on the corporate IT-systems.

In a corporate environment, passwords must at least comply with company password policies, the most common one is the Active Directory Password Policy. This makes guessing extremely hard for a hacker, and after a number of failed attempts, the account locks down and a service desk operator is required to reopen it. This method does not generate enough success for the hacker. In AD, the passwords are encrypted and hashed, so the hackers cannot even use a stolen copy.

Instead, hackers can sometimes get passwords from users through e-mail phishing. Most organizations are aware of this problem and would have implemented a solution to prevent this occurring.

But if you are a hacker and need a password from a specific user (or small user group), how can you get it? Just use your phone and ask for a password!! Key people are not an easy target and will not give out a password through a spear-phishing attack.

Alternatively, the hacker will call the service desk and pretend to be a real user with a user-id. If the hacker is well prepared, he can impersonate the user and give relevant details in the conversation. The service desk is there to help, so odds are good for the hacker. Research done by Group-IB, highlighted a 75% success rate for gaining information when combining e-mails and phone-based calls (Vishing).

For organizations that have a large service desk or an outsourced service desk, the service desk staff might not be familiar with most users by voice or their habits. The hackers can use this as an advantage to get details about the key IT-staff, and even get a new password for an IT-user. This is a black hole security wise for the most critical It-infrastructures and might explain where the hackers get the passwords for the data breaches!

Phishing and vishing are social engineering methods and rely on human interaction. Up to now, the best mitigation has been awareness training, but research shows that good social engineers can still fool some of us.

A robust and secure mitigation is an intelligent IT-workflow to verify the identity of people calling in. This removes the social engineer's most powerful weapon, human interaction, and emotions! We cannot do this for all employees, but we can do it where we have important data and assets serviced by central service centers such as the IT-service desk, the HR-department, and the Finance department. In the verification process, dynamic and contextual information would make it exceedingly difficult for a hacker to impersonate a user. Combine an intelligent workflow with modern tokens like OKTA, DUO, and authenticators such as Google's and Microsoft's and this makes the process easy for users and extremely secure.

If you want to see more facts and statistics on this as well as real life examples of vishing attacks against large It-companies, go to this blog: https://www.fastpasscorp.com/blog/it-departments-targeted-vishing-attacks/

CHAPTER 5

When can a Password for Active Directory be a threat to your corporate IT-system?

The simple answer is: When a hacker has the password! The thing is however, that it's not as easy to get a corporate password, as it is to get a private password!

So how can a hacker in the real world (as opposed to the theoretical world) get a corporate password?

The standard ways for hackers to get passwords are:

- **Guessing**
- **Reuse passwords from other data breaches**

These methods might work very well for private access to WEB-services, but for your Active Directory. In a standard Active Directory Strong Password Policy, AD will lock the account after 3 failed attempts – and then you might get a few tries later. This doesn't work for a busy professional hacker.

Even if you have a password from a data breach from a WEB-system with a corporate user-id, then the corporate password syntax is different. Some users might use the complex corporate password for a commercial WEB-system. But when it is breached hopefully the standard duration of 3 months has expired and the password is no good anymore!

This leaves social engineering as the preferred method for the hackers.

E-mail phishing is well-known. It works, but in general, the hacker can't know what users will react. It is to be expected that IT-staff won't fall for the trick.

If you as a hacker needs the password for an IT-staff to get access to internal tools you have to ask someone else for the IT-staff member's password: The central IT-service desk!

The hacker simply calls the service desk pretending to be the IT-employee and asks for the AD-password, using social engineering methods. Using the phone for this is called Vishing!

OK! In theory it might sound acceptable – but does it really happen?

1. **69% of IT departments** have been targeted by a vishing attack *(Statista)*
2. Criminals use passwords for data breaches in **50% of incidents** *(Verizon DBIR)*
3. **78% of IT Service Desk managers** fear a criminal can get a password from their supporters *(SDI)*
4. **75% hacker success** when combining vishing and phishing! *(Group-IB)*

We even have some prominent examples from the IT-industry: CISCO, Twitter, Microsoft, OKTA have all described data breaches, where social engineering against central IT-service teams were part of the attacks. See more details in this blog: https://www.fastpasscorp.com/blog/it-departments-targeted-vishing-attacks/

What mitigation can prevent this?

Awareness and training are considered the best possible methods against social engineering. The problem is, that the social engineers are experts at this, and our employees are (good) amateurs – it is an uneven match!!

A strong alternative is to implement an intelligent IT-workflow controlling the user identification process and the IT-supporter – not the other way around. If the intelligent workflow includes dynamic and contextual data plus tokens then we have made the task impossible for the hackers. Remember however to remove the privileged rights for the IT-supporters or the hackers might convince them to pass the controls in this way!

An example of an intelligent workflow for end-user verification integrated with ServiceNow can be seen here: https://www.youtube.com/watch?v=xquvM0aDNs0

CHAPTER 6

The Uncomfortable Truth about IT crime against Enterprises

Your next IT-breach will probably start when a "friend" convinces someone else to give away a password. This doesn't require any IT skills!

The facts are probably known to you, but you might not have put the facts together as done here! The reality is that an IT-crime can start simply and by trusted people.

- Most attacks start with a social engineering attack
- Your "Friends" are doing it to you
- They only need a password (credential) to start

You might ask if this is true. Don't take my word for it. Research from the most trusted security companies have found that:

1. **Most attacks start with a social engineering attack**

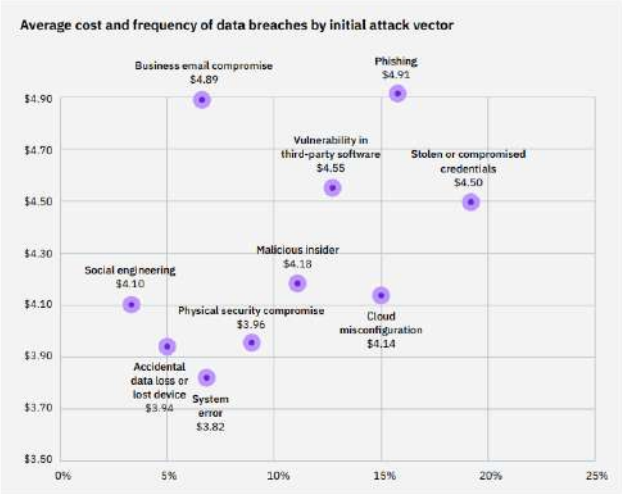


Figure 11: Measured in USD millions

IBM report https://www.ibm.com/reports/data-breach

The sum of Phishing, Social Engineering and Stolen or Compromised Credentials amount to nearly 40% as initial attack vector! It includes spear phishing, vishing and smishing.

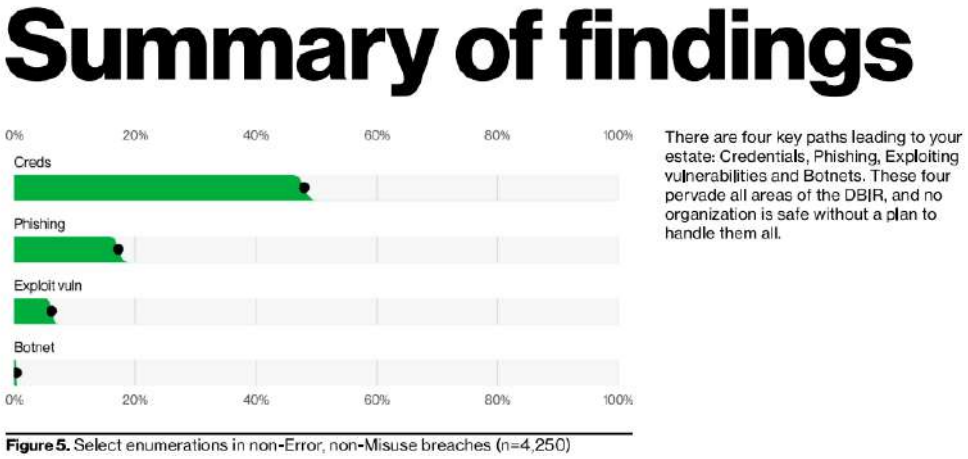
2. Your "Friends" are doing it to you

KPMG: https://assets.kpmg/content/dam/kpmg/xx/pdf/2022/01/fraud-survey.pdf

Organized criminal associations are involved in less than 30%, the remaining individuals you would consider belong to your “safe places”! Your employees and business partners, vendors and customers are involved in most of the fraud and misconduct (KPMG).

3. **They only need a password (credential) to start**

   Verizon 2022 DBIR: stated 50% of data breaches can be attributed to leaked credentials (passwords).



Verizon: https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

Verizon refers to credentials as the means to get to your IT-system. This primarily means passwords.

Many data breaches have occurred where large volumes of passwords have been exposed. This is however always from commercial web-systems. We haven’t seen any examples of a corporate Active Directory being stolen and misused, as the AD passwords are hashed and encrypted.

This is a fact because most companies have implemented Active Directory strong password policy. Hackers might still be able to guess or find a user’s password, but we can expect that most passwords for enterprise systems are stolen because someone has given it away to the hackers. This is called social engineering!

Ask yourself: How well is your company protected against employees and close partners who using social engineering want to steal a password from an IT-user??

How does it happen in reality:

The hackers have different ways to get a real users password:

- Ask a colleague for their password - it might be inside a partner company too: “I need a job done, and if I get access to your account, you don’t have to spend your time on it?”
- Call the IT-service desk and impersonate an employee, calling up from his office-phone: “Hi, this is Joe, I forgot my password – can you give me a new one?”
- Send a phishing email to users and ask them to use their password for some special reason, at a WEB-site you control.

When the hackers have the access they might steal your customer list, your product designs, your money through false invoices. Perhaps they sell it to a real hacker who installs ransomware. Beware that on average it takes 207 days before you discover that you are the victim of a data breach. This means that most data breaches are well hidden and in no way dramatic. Our guess is that a lot of data breaches are never identified!!

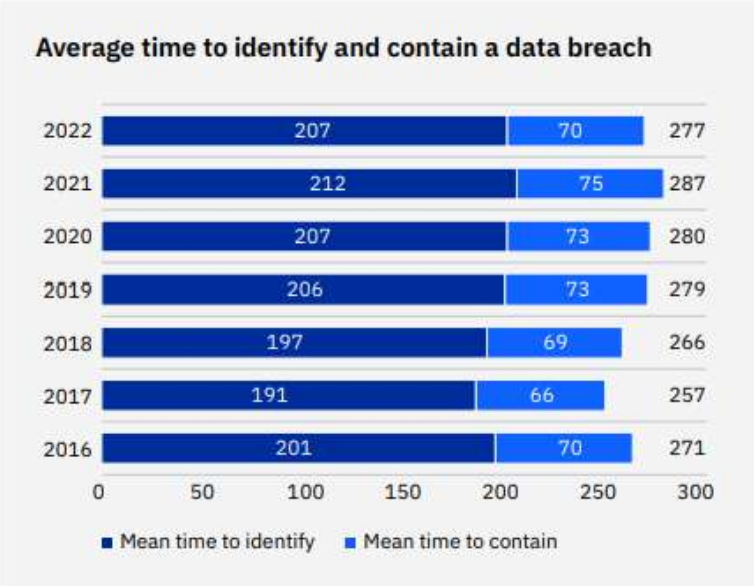


Figure 8: Measured in days

IBM report https://www.ibm.com/reports/data-breach

On average it takes more than 200 days from the attack before it is identified. The fact is that for most IT-crimes the hackers don’t want the victims to know that they have been robbed!

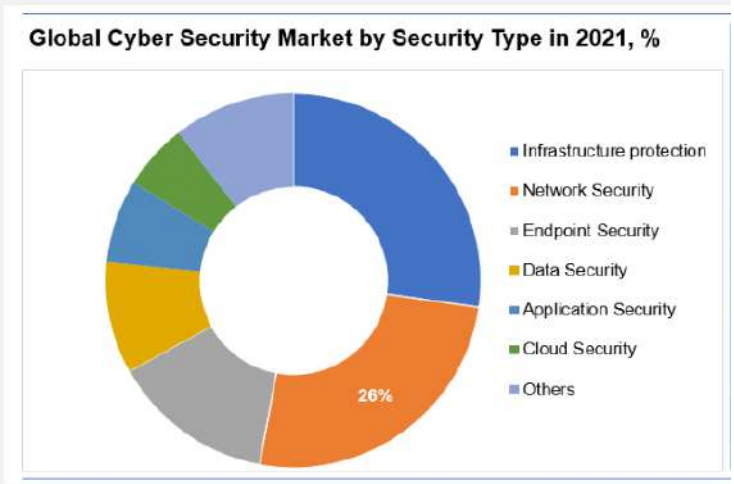
Mitigation:

What security product will solve this? No single product will solve the total exposure! The most important decisions will be in these areas:

- **General awareness training is important**
- **Two-factor authentication where possible**
- **Phishing "filters" as far as possible**
- **Forced Identity Verification workflow for central resources like the IT service desk**

Do you have the right protection to defend yourself against the early steps?

What are the investments in products to protect against social engineering? We don't know as it is such a small amount that it is not even counted. This is from Agile Intel Research:



It doesn't have its own category despite being amongst the most important threats!! This indicates that too little attention has been offered to one of the most critical vulnerabilities: Social Engineering!

Products are emerging now to protect against social engineering and should be considered to complement awareness training. FastPassCorp has a forced workflow for user identity confirmation for central resources, where employees/partners call to get different types of assets, as a password from the central IT help desk [Identity Verification Manager.]