How to start with CVD

"All ins and outs about CVD and how it can help protect you and your business' information"

zerocopter

zerocopter.com | info@zerocopter.com

Introduction

Four billion devices were added to the internet-of-things in the past years. With this increase in the number of devices comes a rise in the complexity as well. The classic example goes that a standard smartphone nowadays is thousands of times faster and hundreds of times more complex than the computer that sent the Apollo 11 rocket to the moon. This ever-increasing complexity affects the ultimate structure of the internet, impacting all that use it. As the rapidly growing number of complex devices are added to the internet, the number of attack surfaces for cyber criminals to target also grows. These attack surfaces continually inflate in size and complexity, especially as business becomes more centred in the digital world.

On top of the volume of devices, the speed at which software and updates are released is increasing as well. In the past, releases would be few and far between with relatively large changes happening at once. Now, these can come every day, with many smaller changes being issued within the same time period. These releases can introduce other risks.

For example, more content can lead to an increase in attack surfaces. At the same time, it can also allow fast and effective changes which can help maintain system security.

Businesses are heavily influenced by changes in cyber security: any company which stores their customers' information has intense pressure and responsibility to keep it safe. The scarcity of in-depth security knowledge in most development teams makes it impossible to create a system completely secure from the start, so, after launching it, many

businesses have to roll with the punches as they come.

To adapt to the quickly evolving cybersecurity landscape, businesses have started to apply their own creative ideas to strengthen their defences. One of the largest and best defences against criminal hackers is to use hackers themselves. White hat or ethical hackers have risen to prominence because of their added creativity and grasp of attacking systems. They can relate the process of how a cyber criminal might attack a system with how a business might defend it. That'll help build strong walls against cyber criminals.

Ethical hackers (although we refer to them as researchers because they are the ones that research your scope) can provide various beneficial services for businesses, including penetration tests and bug bounty programs. They can even submit external vulnerability reports using CVD, Coordinated Vulnerability Disclosure. If you don't know much about CVD or how it can help protect you and your business' information, do not worry, that is what we will discuss in this guide.

What is CVD?

What is disclosure?

Disclosure is the transfer of information from an external source to a company or organisation, in this case regarding the security of IT systems. When a researcher or criminal discovers a vulnerability, there are four ways they can handle the information.

1 **Non-disclosure** is one method in which the external researcher or criminal that discovered the vulnerability keeps the information to themselves. This can be for multiple reasons, whether it be because they plan to use the information as leverage or because they fear legal repercussions when sending in a report. A company outlining preconditions and agreements can help convince the latter situation to turn in the information responsibly.

2 **Limited disclosure** is the next form. With limited disclosure the researcher or criminal only releases a small or limited amount of information about the vulnerability to a limited number of parties. Limited disclosure puts pressure on the company to quickly fix the vulnerability because it can put customer or company data at risk of exploitation. Luckily, this form of disclosure is contained to the few parties involved in the information transaction.

3

Full disclosure is another form of disclosure in which the researcher or criminal releases the vulnerability information publicly. Though this provides the company with direct information about the vulnerability, it also puts them at risk if they cannot resolve the issue fast enough. Criminals can easily access the vulnerability information and exploit it as long as it's not fixed; bad news for companies.

4

Responsible disclosure, or Coordinated Vulnerability Disclosure is the final and most important form of disclosure. With responsible disclosure, the researcher directly contacts the company or multiple companies about a vulnerability which affects their systems. The information isn't shared publicly until the vulnerability is fixed. This form of disclosure provides the best protection for companies against exploitation or data leakages. A CVD program protects both the company involved and the researchers submitting the reports.

What is CVD?

CVD, or Coordinated Vulnerability Disclosure, is a program which focuses on contributing to the security of IT systems for companies, organisations or any group that want to strengthen themselves by targeting vulnerabilities. A CVD policy allows companies to indicate that they are open to receiving vulnerability reports from external researchers who may have stumbled upon a system fault and that they have a set course of action in the event a report is submitted.

A bit of history

In the Netherlands it all started back in 2013 when the National Cyber Security Centre (NCSC) published a guideline that would pave the way for what's nowadays the Coordinated Vulnerability Disclosure policy. Since then NSCS constantly encourages public and private entities to implement such policies. Why? Because NCSC believes in a trust based cooperation within the community that will make the digital world more secure.

2013

NCSC

published a guideline that would pave the way for what's nowadays the Coordinated Vulnerability Disclosure policy.

Before 2013, this disclosure process was still a criminal one. In order to regulate that, the Coordinated Vulnerability Disclosure policy was created to set up some ground rules, do's and don'ts between reported parties and organisations. Besides the fact that it's meant to encourage a responsible disclosure of vulnerabilities, it also has the purpose of stopping the involvement of legal parties for each reported vulnerability. This means that if the reported party will follow the boundaries within the policy, there will not be a criminal complaint.

Nowadays, more and more countries around the world are establishing Coordinated Vulnerability Disclosure policy in order to make the digital environment more secure.

Preconditions and agreements

Preconditions can be laid out so companies can clarify how they would prefer external reports to be submitted, and how they will process and correct the discovered vulnerabilities. In addition, it is important for external researchers and companies to lay out a set of agreements and follow them to allow a smooth transaction of information, as well as, in the end, benefitting both parties involved.

An important aspect of any set of established preconditions is an agreement in which the company promises not to report any external researchers who submit information. This allows the external researchers to present their vulnerability reports, and thus help the company, without fear of legal action. This ultimately benefits the company, even if accepting that researchers may be researching your IT systems can be difficult.

Advantages of CVD and starting building a relationship with the hacker community

Vulnerabilities are an integral component of computer software. It is impossible to develop a program which is impervious to tampering with. A program can be built with an endless number of protections and security measures, but there will always be some form of weakness. For this reason, security flaws should not be seen as shameful but as a source of inspiration to build more robust defences. Starting with CVD can help awaken the needed motivation as well as help form a solution. Here we will discuss 7 of the biggest advantages of starting with CVD and working with researchers.

zerocopter

A continuous solution for a continuously changing world

In the last decade alone, the pattern of software releases has changed dramatically. Ten years ago, software updates and new programs may have been released a few times a year. Updates were coupled with heavy testing before release and drawn-out release schedules. Now, software is released almost continuously. This is great for business and boosts company responsiveness, but can leave the software not thoroughly tested. A CVD provides a solution for this by providing constant and dynamic feedback on the security of your systems, regardless of how fast your releases are.

CVD programs provide a safety net against any errors in your systems that may have resulted from the commonality that humans make mistakes. When updating a system, especially on a release deadline, mistakes are bound to be made. Flaws can be identified and corrected quickly, taking pressure off developers. Common flaws, like Business Logic Vulnerabilities, arise from the design or implementation of a process in a system.

Diagnose more of your bugs

Finding security issues or bugs in code can be a difficult task, especially for those who write it. In the same way, a new newspaper article is passed through multiple hands and checked over numerous times before being published, code and software can benefit from new perspectives both before and after the release. Initialising a CVD program can provide additional and safe perspectives to help uncover issues in a system that may have gone unnoticed by the developers. Researchers utilise creative and abstract strategies to find holes in a system's code which would be very difficult to discover without that additional set of eyes.

For example, between 2020 and 2021, the top most found vulnerabilities under the Zerocopter CVD programs were: Security Misconfiguration, Cross-site scripting (XSS), Information Disclosure, Open Redirect, and code Injection.

Stay ahead of cyber criminals

Setting up a CVD program gives you access to a global team of researchers who work towards strengthening your systems, though not directly working for you. A worldwide network of researchers can uncover more extensive and impactful vulnerabilities than security or development teams could in the same amount of time. The potential for valuable information can push you ahead of any criminals that may be looking for the same vulnerabilities.

Show the public that you are open

Publicly showing that you are prepared to receive reports via CVD shows your customers that you are open and devoted to keeping their information safe. Consumers may put more trust into the security of your online presence if researchers, which aren't part of the company, dig through the code and point out any flaws and imperfections. Openness conveys confidence. Consumers value confidence when choosing who to trust their information with.

zerocopter

The advantages of working with researchers

Researchers have experience in the field of digital breaking and entering. Their expertise lays in looking at a problem, finding a small error or mistake, and cracking it open like an egg. Criminal hackers use this ability to take, steal and manipulate, which can be scary and intimidating. Development or security teams prepare for attacks by setting up layers of security. Mistakes are usually made, however, which can easily be taken advantage of.

Those teams try to think like a criminal hacker and try to prevent those specific attacks. By working with researchers, you can smooth out the imperfections that a development or security team may not even think could be an issue. Researchers perform the same breaking and entering that cyber criminals do, but instead of taking what they can, they make the bed, clean the counter and directly inform the staff about an unlocked door.

Giving a researcher the go-ahead to intentionally break into your systems can be very scary, but the benefits heavily outweigh the downsides. Working with researchers helps prevent unexpected intrusions and helps prepare for future cyber attacks

Train as you go

After starting with CVD, you will get reports on your system's most significant and, sometimes, smallest vulnerabilities. With those reports, developer and security teams can refine and polish the system to remove those vulnerabilities. While fixing those weaknesses, your teams will also get additional experience and training on what to pay attention to next time they update or add to the system.

Experience is the name of the game when working with researchers. From their own experience in cyber security to the new experience your development and security teams will acquire, starting with CVD will help you improve. Though working with researchers can appear dangerous, their goal is the same as yours: **to help improve your systems and set up a safer environment for your business and your customers. Because the researcher can very well be your customer.**

Save on security expenses

Incorporating a CVD program, as well as establishing preconditions and agreements, can help replace more costly system-check methods. CVD is a low-cost method to identify vulnerabilities within your systems, and with the work of a strong development team it can also be a solution. This helps save on money spent finding the problems and allows for more capital to be invested in forming a solution.

Though disclosure is beneficial, it's important to keep in mind that it cannot completely replace other system checks due to reliability. Even if you open up the scope in which researchers can investigate your system, you may still have times when no researchers submit reports, and you would need to check for vulnerabilities with other methods. Make sure you have a baseline with IT security measures and check it in a structured way, such as regular pentests.

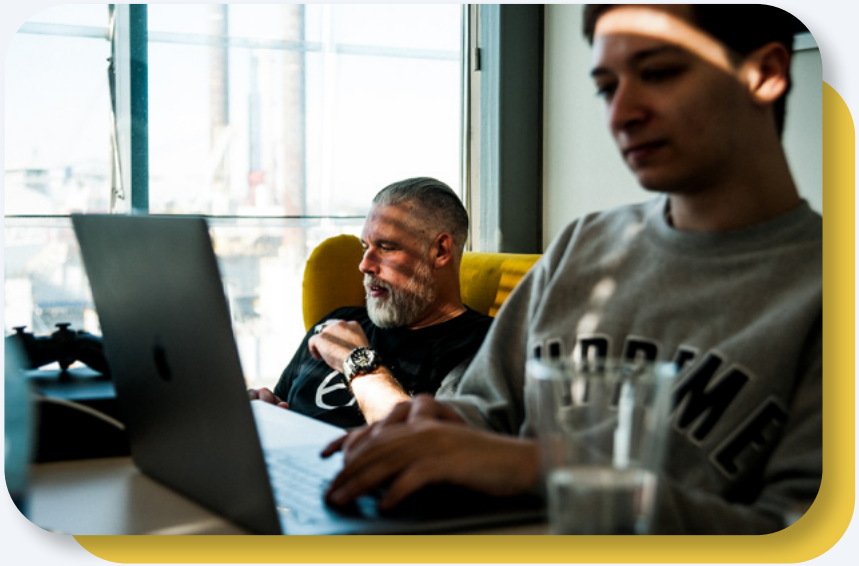
CVD integrated with other programs

There are many ways to test the security of an online system, and all of them can provide valuable information on how to improve and strengthen the system against cyber attacks. Each program or method has its upsides and downsides; here, we will discuss how a few of these methods can be combined to create more comprehensive and in-depth security techniques.

zerocopter

What is a pentest?

A penetration test, also known as a pen test or pentest, is an authorised and simulated cyber attack aimed at finding vulnerabilities in a system. In addition to finding weaknesses, a penetration test also considers the strengths of a system, allowing the production of a full risk assessment. A penetration test can help determine whether certain defences within a system are sufficient to fend off an attack or if they fail as a result.



There are two forms of penetration tests: black box tests (in which the auditor is given the bare minimum of information about the company) and white box tests (in which the auditor has access to system information and company background information). More realistic situations settle between these two types of pentests. The in-between is called a grey box test, where a small but realistic amount of information is given to the auditor.

Sometimes, to perform the test, hypotheses are made about where the system may have weaknesses based on system information with the scope of the test being guided by those hypotheses.

CVD and Pentests

Pentests are valuable because of the amount of specific information they can return on the security of a system. Additionally, pentests go very deep into a particular scope of a system. The information received can be valuable for strengthening, fortifying, and correcting vulnerabilities. Pentests, however, are relatively costly, and because they go deep, may not be able to cover the entire scope (at least not for a reasonable price). Also, pentests are usally done by one or two testers, with their own expertise.

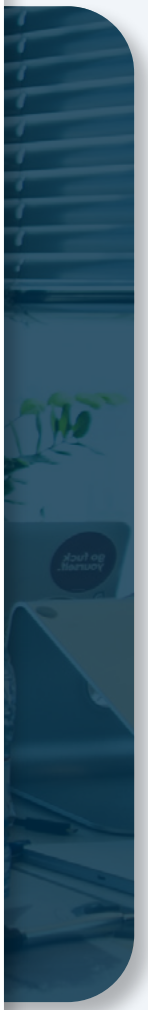
That is where disclosure and a CVD policy can come in handy. A CVD can invite a large number of researchers with different expertises on where to look for vulnerabilities. The reports from external researchers can be compiled and analysed to find which parts of the system have the most vulnerabilities and impart the greatest risk for data security.

A CVD policy which encompasses a large part of the system can get you valuable information on which parts of the system need the most attention, and which parts of the system are worth investing penetration tests in.

What is a Bug Bounty program?

A bug bounty program is a competition in which researchers are invited to look for and disclose any weaknesses in online or network environments. For each bug found, the hacker receives a prize (bounty) based on the severity of the weakness.

There are two categories of bug bounty programs: public and private. Public bug bounty programs are open to everyone. Private programs require organisations to invite ethical hackers to participate. Despite public programs yielding the best results - because they attract a considerable amount and wide variety of ethical hackers - we are a fan of and specialise in private bug bounty programs. We use our network of experienced and vetted security researchers to find vulnerabilities. Zerocopter specialises in private programs because they grant our clients the control and the organisation to effectively identify and fix vulnerabilities.



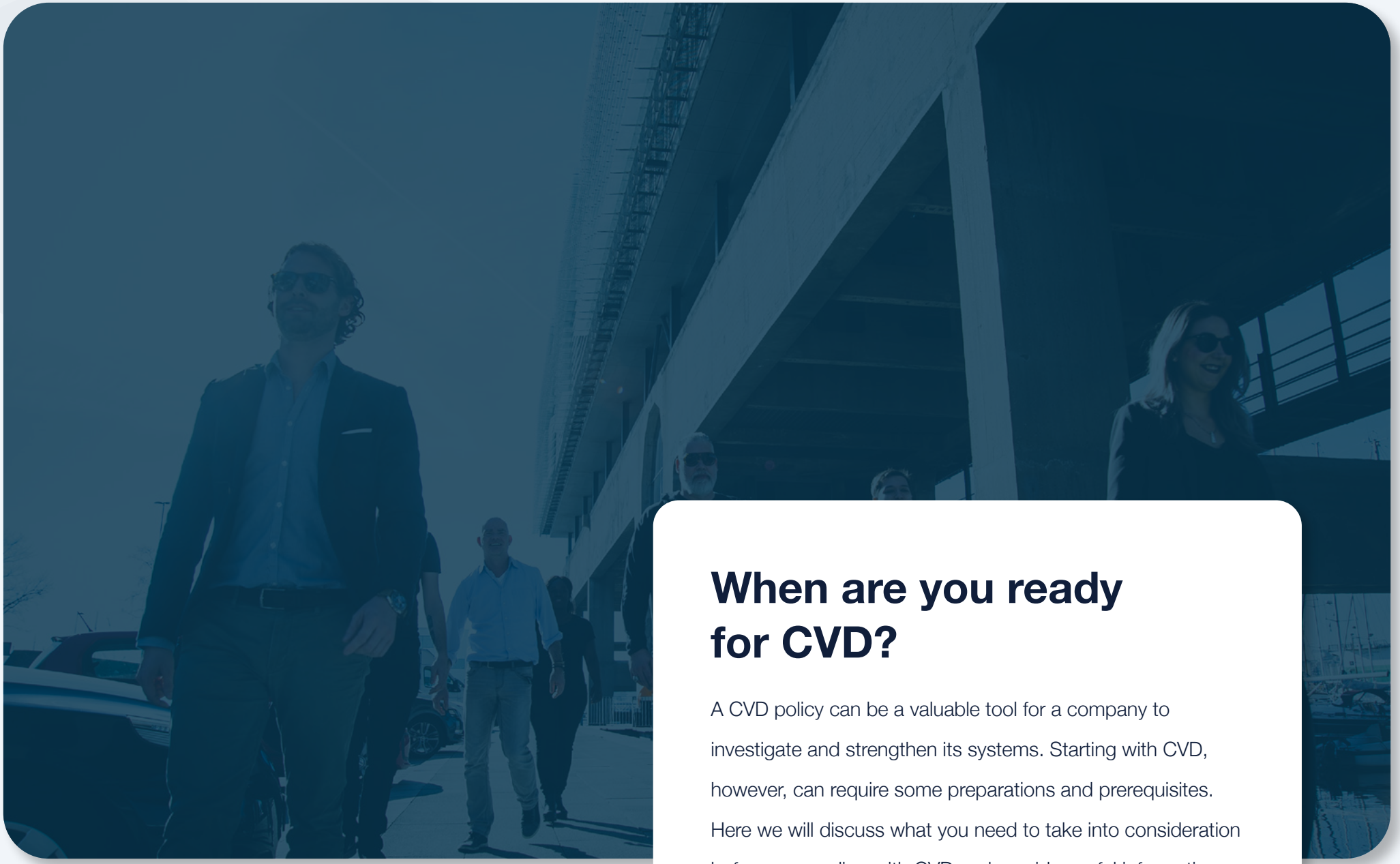
zerocopter

Bug Bounty and CVD

CVD allows for easier disclosures of vulnerabilities from external parties, which plays nicely into the core of bug bounty programs. Successful bug bounty programs are essentially organised CVD events with extra motivators. CVD is a passive agreement which results in vulnerabilities being discovered and disclosed without punishment. Bug bounty programs, on the other hand, ask researchers to find vulnerabilities and get paid for reporting them, also without penalty.

In a way, a bug bounty program is a form of CVD which more directly motivates researchers to find and disclose vulnerabilities. Combining the two can be invaluable to an organisation that strives to strengthen their security without directly hiring experts or without taking actions against researchers who want to disclose vulnerability information.

A bug bounty program can bring in lots of vulnerability reports. The programs can be controlled in size, which deviates from the basic principle of CVD: CVD is public. The two programs go hand-in-hand. For more information on bug bounty programs and how you can start your own, see our **whitepaper about Bug Bounty Programs.**



When are you ready for CVD?

A CVD policy can be a valuable tool for a company to investigate and strengthen its systems. Starting with CVD, however, can require some preparations and prerequisites. Here we will discuss what you need to take into consideration before proceeding with CVD and provide useful information about what to expect if you decide to implement one.

zerocopter

Maturity and active security

A CVD policy requires mature and active security behaviour to avoid getting overwhelmed with reports. The first and largest step to ensure that your organisation is ready for a CVD policy is to self-assess your current security situation and predict how it would perform after introducing a CVD policy.

Generally, any organisation that stores or uses data and requires a secure system will receive vulnerability reports before incorporating a CVD policy. These reports can also hold valuable information. However, they can be untrustworthy because they do not directly follow any set agreement or preconditions. If your organisation receives external vulnerability reports from researchers and does not already have a CVD policy with preconditions and understood agreements, it would be valuable to consider incorporating one.

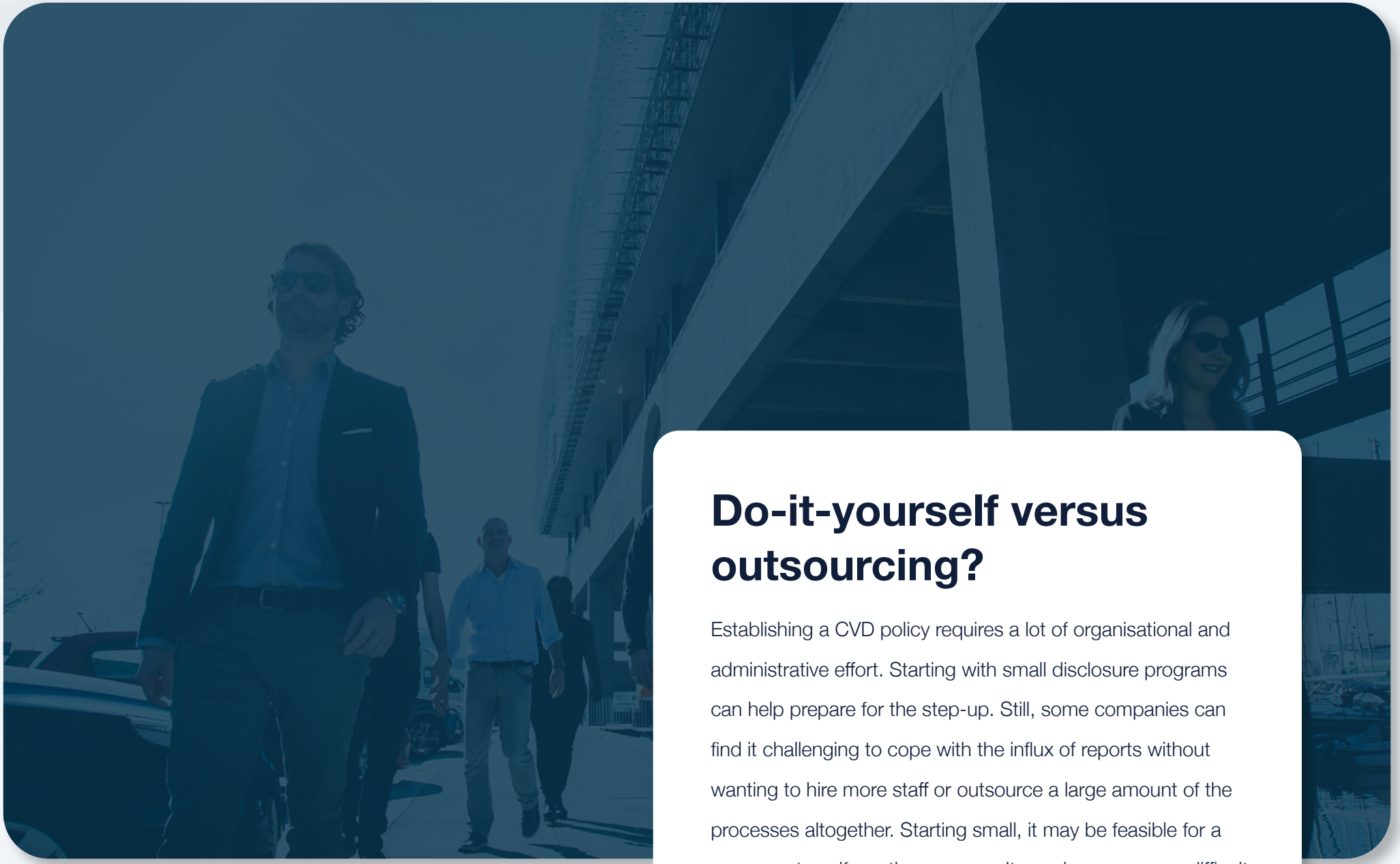
Even if your organisation doesn't receive reports, it can be very beneficial to incorporate a CVD policy.

Receiving reports

It is important to have a set method to receive and process reports. Organisations and security teams can quickly become overwhelmed if they are not prepared to receive a large number of reports within a short amount of time, especially when first incorporating a CVD policy. Once a policy is established, researchers may dig through the designated scope and find many small, but still significant vulnerabilities. The ability to take in reports and promptly respond to them while staying organised is essential. Taking in reports may be as simple as having a set email or form for researchers to submit vulnerabilities.

Think about preconditions, issues not to waste time on, and other rules

Establishing rules will be the first and most important step when establishing a CVD policy. Determining where and how researchers can explore your system and pick out vulnerabilities is paramount to improving your security. This keeps the data and information privacy of your company and your customers safe. Also, you can mention certain thing to be off-limits. Like ordering for a large amount of money. Of any known issues that you've already decided to accept the business risks on. Before incorporating a CVD policy, setting rules and boundaries should be an in-depth process that analyses your system's structure and what you hope to achieve from the policy. Afterwards, a CVD policy can become a evolving policy: you might want to inform research to not waste time researching for a larger problem that turned into a bigger project.



Do-it-yourself versus outsourcing?

Establishing a CVD policy requires a lot of organisational and administrative effort. Starting with small disclosure programs can help prepare for the step-up. Still, some companies can find it challenging to cope with the influx of reports without wanting to hire more staff or outsource a large amount of the processes altogether. Starting small, it may be feasible for a company to self-run the program. It may become more difficult as the number of reports increases, however.

Keep it in the company

If a company is adamant on running their own CVD program, they need to keep in mind the importance of staffing. When beginning a CVD program by establishing a policy, a sudden and large influx of reports can quickly overwhelm a small or unprepared team. Without an experienced team, your entire program may begin to fail. Teams should be prepared and patient enough to take on the challenge of categorising, sorting and resolving a large number of vulnerability reports. If the program fails, researchers will start to find other organisations with better resolution processes and leave your systems untouched and therefore unchecked. Also, you need to know how to provide payments to these researchers.

Outsourcing the management of handling reports

It may be less costly for your organisation to outsource a large amount of the work required when managing external researcher reports. Outsourcing to a company that specialises in the management of and payment for vulnerability reports, such as Zerocopter, can reduce the required administrative and communicative workload for your organisation, allowing you to focus on resolving vulnerabilities.

Outsourcing can handle a wide range of organisational and communication processes which are tedious and time consuming for self-managed CVD programs. Some of these processes include:

- Creating the policy
- Triage of reports
- Arranged payouts and communication with researchers
- Reduction to a single point of communication
- Automatic sorting of reports, letting you access the
- most pressing issues first
- Automatic duplicate removal

Some of the processes above can be solved with APIs, but the experience from outsourced companies can be invaluable. Experience is an essential factor to consider when deciding to self-manage or outsource your vulnerability report pipeline.

Quick Guide: How to set up CVD

The Dutch National Cyber Security Centre (NCSC) recommends five steps to prepare for and create a CVD policy. Here we will go through those steps and provide some recommendations from our experience.

1

Establish the Rules

Setting up rules for researchers to follow, including preconditions and agreements, will make processing reports safer and faster. To begin, even though is not mandatory, you can set up the scope in which the researchers can work. Setting a scope can include which URLs and system components can be investigated without repercussions. Here you can also establish which portions of the system are out of scope to researchers.

Other important rules to establish are what is allowed and what is not, such as how researchers should handle vulnerabilities if they do not want to be charged for entering your systems. This can be outlined in a ‘Do’s and Don’ts’ section. This section can also focus on how deep researchers can enter and manipulate your systems to find vulnerabilities. For responsible disclosure, outlining what researchers are allowed to do is one of the most important steps in integrating a CVD policy and program.

You will also want to establish what you will be promising, such as your response time and how you will be handling the researchers’ information. Based on your promises... developing trust is important in attracting researchers, and sticking to those promises projects a good light on your company.

2

Make Capacity Available

Ensure that you have the staff and organisational capability to begin the program. If needed, you may have to set up a way for reports to be received and processed. Systems to help triage reports and mark which ones qualify for your program are also essential to establish before integrating a CVD policy. Adding additional staff members may be necessary because it is shown that a company receives more vulnerability reports after establishing a CVD policy.

This would be the point to consider whether outsourcing to a company like Zerocopter would be beneficial. Outsourced programs get the benefits of triaged reports, payout arrangement, communication simplification, automatic report sorting, duplicate removal and more.

3

Receive Reports

Once you begin receiving reports, it is paramount that the reports are delivered to the right team. From there, the team can contact the researcher and outline how long the vulnerability will take to address. Generally, hardware vulnerabilities take longer to fix than software vulnerabilities and should be accounted for.

Having everything organised is vital in establishing a CVD policy. Reports can easily be lost if not appropriately handled. Having an organisational structure established before publishing a CVD policy will help maintain an efficient and effective report processing program.

4

Resolve the Problem

Communication with the reporting party once the company starts to remedy the vulnerability can improve the companies reputation and encourage further work on their systems. If a vulnerability is too difficult to resolve or involves

costs high enough, a company can decide to accept the vulnerability as a risk and communicate that to the reporting party.

Researchers expect prompt responses to their reports, thus resolving vulnerabilities should be a rapid and in-depth process. Development teams can only work so fast of course, and researchers understand that. Communication with the reporting researcher can help advertise your CVD program and help resolve vulnerabilities. The researcher may even have ideas on how to remedy the situation.
vulnerabilities take longer to fix than software vulnerabilities and should be accounted for.

5

Reward the Reporting Party

Determine if and how to reward (either with swag or money, or both). How much will the payment be? How are your going to handle these payments? What swag would you like to offer? Also, think about what you need to take into account. For instance, it must be possible and payable to send the swag or payment abroad. Or it must fit your organisations mission and vision. Examples of swag are a hall of fame for recognizing researchers or a letter of appreciation.

Providing a reward to researchers who followed the CVD policy can develop an air of trust and responsibility. Additionally, researchers will want to continue to help strengthen your systems. Over time you can develop a loyal group of researchers working to keep your company's and customers' information safe. Concluding the interaction between researchers and organisations can also help the IT community, especially if the disclosed vulnerability appears elsewhere.

Summary

Establishing a CVD policy can be an incredible asset to your organisation, especially as our world becomes more complex, and cyber criminals get more and more opportunities to do their work. By setting up relations with researchers, you build a team that works towards helping you be as secure as possible while keeping an eye on your vulnerabilities. With responsible disclosure, you get insights into how you can improve your system's security while showing your customers that you genuinely care about their information security.

Starting with CVD can be difficult. You need to ensure your systems are prepared and you have enough staff to process and remedy the vulnerability reports you will receive.

But we can help! Zerocopter allows you to set up your own Coordinated Vulnerability Disclosure program, making it easy for people to report an issue. And not only that: we go through the alerts for you. This way we collect, summarise and prioritize the alerts for you and you'll know what to focus on.

The benefit of improving the security of your systems, however, is well worth the extra effort.

Luckily, there are ways to make it less difficult: like Zerocopter, which can help you organise and simplify the reporting process.

If you are interested in how Zerocopter can help you with CVD, download our brochure.

Learn how Zerocopter helps security

Download our brochure

Contact

Monday - Friday

9:00 - 18:00 CET

+31 20 261 67 43

info@zerocopter.com

Location

Kraanspoor 50

1033 SE Amsterdam

The Netherlands

Sylviuslaan 2

9728 NS Groningen

The Netherlands