Colophon

Pentesting according to the methodology for information security research with audit value

Compilation and editing: Brenno de Winter

Cover design: Mischa van Geelen

Interior design: Brenno de Winter

Advice and support: Hans van der Looy

Non-fiction: Technology & Society

Publisher: De Winter Information Solutions

Nov. 22, 2024, first printing, NIS2 edition

Foreword

Whether a network, system or software is secure is difficult for many people to portray. After all, what is considered secure? There are official certifications that look at policies and procedures, but technical testing remains a complicated issue. How should you interpret a report if there is no clear framework? What assurances do you have then? And how can a technical investigation properly serve as input for a certification? After several incidents in the industry, many experiences in doing (technical) research on products, but also on incidents, it is clear that we need more guidance.

With something physical like a home, the measures are easy to check from lists (do you have exterior lighting, certified locks, reinforced door hardware, an alarm system, camera system and other things). With networks and software, the playing field is more complex, but not substantially different: there are several lists of surveys (checklists) to go through. It's less magic than is sometimes claimed in the industry. But what are tests you want to have gone through at a minimum to have some honest idea of the level of security on the assessed product or platform?

This methodology was developed for that purpose. The goal is clear: a technically focused investigation must actually bring something to the table that provides assurances. Not only for the direct recipient, but also, for example, an auditor must be able to trust that this research answers the questions. Therefore, the methodology is designed to make each step notonly replicable but also irrefutable. Reproducibility and irrefutability mean that there is some audit value. It is clear what was investigated, how it was done and what the result of that investigation is, with the underlying evidence available to reproduce investigations or make them available to regulators, for example, as required by the NIS2. All in all, it provides a reason why you have confidence in a product.

Central to the methodology is that research is focused on factual investigation based on important and relevant (international) standards. We bring that together for research, reporting and determining the severity of a finding if imperfections are found. By doing that uniformly we are talking about the same thing, a lot of emotion is taken out of the debate and a discussion can be based on facts.

It not only provides information, but steps also to take, but a guide to properly assess information security research. We define procurement requirements, process diagrams and standard reports. Where possible, these are incorporated into relevant tools. That way we don't exclude anyone and compliance with the methodology is not complicated, and we banish all magic to achieve compliant research.

Going through the necessary requirements can only work well if questions and answers are well aligned. From question to review of the final report, the methodology provides the necessary information and models. Where there were gaps, as with many legal aspects, we filled them in as best we could. In this way, this methodology provides guidance for an honest, objective picture of the research carried out, with the report providing color to the requirements that the European legislator increasingly imposes on information security.

The information security examination with audit value revolves around a number of certainties, which can be dissected from the examination:

1. **Clarity in Expertise:** Based on certification, it is evident that the study was conducted under the supervision of someone who is adequately trained.
2. **Clarity in Process:** The process is well-defined and fully outlined, providing clear guidance throughout.
3. **Clarity in Completeness:** According to the relevant standards, all required tests have been performed. If any tests are not applicable or could not be conducted, that has been documented. This ensures that a comprehensive examination has taken place.
4. **Clarity in Context:** Based on the available information, the context is clearly defined, including what information is or is not available.
5. **Clarity in Scope:** It is explicitly clear what has been investigated.
6. **Clarity in Research:** The research conducted is clearly outlined and is appropriate to the product being evaluated.
7. **Clarity in Evidence:** Research evidence is available to ensure reproducibility by others, thereby adding audit value and verifying that the research was properly conducted.

8. **Clarity in Findings:** Findings are communicated consistently and as objectively as possible, addressing identified issues, their impact, and potential solutions.
9. **Clarity in Standards Followed:** International standards were adhered to during the information security research, ensuring clarity regarding the minimum requirements for the research conducted.

This document represents the culmination of extensive knowledge and insights gained from various incidents. As the field of information security continually evolves, this document will need to be updated regularly to reflect new practices. For now, it provides a solid foundation to guide you. Sincere thanks to all the bright minds who contributed to its creation. Best of luck as you move forward!

Table of contents

Colophon 1

Foreword 4

Table of contents 8

How it all began 9

The goal of Miaw: to be in control 12

The broader picture 16

The methodology 19

The CCV pentest seal of approval. 22

Process of a pentest investigation 25

The standards from the methodology 38

The report 50

The record 52

Legal aspects of pen testing for clients 55

Sample questions clients 106

How it all began

Brenno de Winter

A client of mine wants to purchase a service from a vendor. There are some risks if security turns out not to be in order. With the request to perform due diligence, at some point security testing comes into the picture. In this case, that is the penetration test. In consultation with the vendor, a problem arises: they are not allowed to provide the research from their researchers to me. And with that, there is nothing. The supplier understands that with that, there are going to be insurmountable objections, and the deal is off the table. It surprises me, because the very research that should have been a brevet of capability is now held hostage by the supplier's supplier.

Eventually, an interim solution emerges. I am allowed to read the test at the supplier's office. But as I read through the pages, something struck me. Something is still missing. The scope is not quite correct and there do appear to be findings. Long story short, I can't write down that it's right and without the nuance (because confidentiality) it's not right for my customer, the buyer. Once again, we are held hostage by the investigators. My suggestion is: fix everything and run another test. Perhaps by another investigating party. It became a very expensive joke, but in the end it worked out and the service could be taken. But for me it was a warning. Something is going on with pen testing.

That feeling was reinforced when I had a customer who was the victim of a ransomware attack. It didn't take long before a penetration test was found. That very document examined infrastructure. Oddly enough, based on the document, you would never conclude that anything would be wrong with the technical environment. Not long after that, another painful thing became clear: based on public sources, you can rebut determinations made by the investigators cuttingly. The story on paper was not in line with practice, and thus the question is reasonable: What else is wrong?

With another customer, there was a penetration test, which only showed the findings. When this client was hacked in a simple way, the question arose: why is this not listed among the findings? This is so obvious. Nowhere in the report did it say what exact tests were performed. And when I thought about it, neither were the earlier tests. In the first case because it was a trade secret and in the second case because they clearly had a skilled base problem. But clearly the reporting did not provide what it was supposed to provide.

Then came the moment when, in the corona crisis, I had the responsibility to commission pen tests on CoronaMelder, the Dutch COVID19 contact tracing app. The results had to go to the House of Representatives and be part of the public debate. The last thing you want then is not to have done necessary tests, errors in reporting and cause for debate about opinions of investigations. This is why uniform standards were quickly seized upon. A testing guide that is fully run down, uniform assessments of findings and, above all, a report that you can say provides assurance rather than a list of errors.

That approach turned out to work. We were more in control, had visibility into what and how had been investigated, how the results had been discovered. This was followed by more applications and coronate tests to prove that they were secure enough. The process of testing whether work had been done according to open rules also provided a fair measuring stick. In all cases, the penetration test was treated the same. It caused some struggles in the beginning, because for the testing organization it became clear how it was being tested and was also checked. But the important thing was that it worked.

After the Covid period, it was clear that this was an asset to take to the concern of the Ministry of Health, Welfare and Sport. Because regulations increasingly demand to be in control and to be able to prove it. The penetration test is an important part of many standards frameworks. That is why the methodology for Information Security Research with Audit Value or Miaw for short was created. This did require an additional component: that audit value or testability. We do this in the process report, in which an auditor looked at the content of the test, the completion of the process, the information provided and especially its correctness: does the pentester really have the certifications, have the tests been completed, is there underlying evidence, what the findings are and how are they uniformly graded? Miaw was born.

The goal of Miaw: to be in control

Brenno de Winter

The importance of well-executed penetration testing (pen testing) is becoming increasingly clear as legislation, such as the NIS2 (Network and Information Security Directive) that culminates in the Cybersecurity Act and the upcoming CRA (Cyber Resilience Act), places more stringent requirements on organizations to prove that their systems are secure. Both the NIS and the CRA require organizations to be able to demonstrate that they are "in control" of their cyber security. This includes not only being in control of their risks but also being able to support this with concrete evidence. Article 15 of the NIS2 Directive explicitly emphasizes that organizations must be able to provide the underlying evidence in an audit.

Why is a well-executed pen test essential?

A pen test is a methodical test in which hackers attempt to find and exploit vulnerabilities in a system. This helps an organization to gain insight into where the weaknesses are and how they can be strengthened. Not all pen tests are created equal. A poorly performed pen test can lead to a false sense of security: if important parts of the infrastructure are overlooked, the test is not sufficiently thorough, the recipient may feel secure while significant risks still exist.

Performing a pen test without a clear and documented methodology may result in failure to identify certain risks. For example, a common mistake is conducting a pen test without paying attention to advanced attack techniques or insider

threats. As a result, only the surface is tested, but complex vulnerabilities remain hidden. This could make an organization vulnerable to ransomware attacks, for example, as in the case of the Hof van Twente municipality, where a lack of effective security led to serious disruptions. So being in control means not only performing a test. It also means also being able to demonstrate what has been tested and why.

Legislation as a guiding framework

The NIS2 directive, which is mandatory for vital sectors such as energy, transportation and healthcare, requires companies to regularly test and audit their systems to demonstrate that their security is in order. Showing underlying evidence, such as test results, is mandatory. The upcoming Cyber Resilience Act is going to tighten these requirements even further. This means that organizations must not only test for technical vulnerabilities but also meet compliance requirements set by standards frameworks such as ISO 27001, or industry standards such as NEN 7510 for healthcare.

The CRA will force companies to be more transparent ov the security of their systems. This means that penetration tests must not only be performed to standards that provide insight into what was tested, but the results must also be verifiable and reproducible. Management must be able to prove that each step in the process has been completed and that all findings have been recorded. This not only helps with compliance with legislation but also reinforces confidence in the organization's overall security posture.

The importance of transparency and reproducibility

Performing pen tests is only part of the story. Transparency and accountability are just as important. When a pen test is performed, management must be sure that the testing methodology is well documented. This means that testers must not only produce results but also be able to show how they arrived at those results. A clear methodology, such as the OWASP Testing Guide, is essential to ensure that all aspects of security are covered.

The procurement of the pen test should therefore be a conscious choice, with clear agreements made in advance about the scope of the test and the methodology to be followed. This ensures that management gets a clear overview in the report of which risks have been tested and which measures need to be taken. This allows you to make correct decisions and remain compliant with legal obligations.

Being in control of a pen test means that as an organization you understand not only what was tested, but also why it was tested. It means that you can be transparent about the testing process, validate findings and demonstrate that you are in control of your security risks. This is not only a legal requirement but is a critical element of good business practice in a world where cyber risks are constantly evolving.

The Role of Miaw

With the Methodology for Information Security Testing with Audit Value (Miaw), we give a color to this need. It provides a structured approach to penetration testing by ensuring the

reviewability of the process and outcomes. Miaw ensures that penetration tests are conducted not only from a technical perspective but also based on a standardized methodology that ensures reproducible results. This methodology emphasizes transparency, scope clarity and validatable findings, minimizing the risks of an incomplete or improperly conducted security review.

The added value of an auditor's process report is crucial. He or she not only reviews the technical execution of the penetration test, but also validates the process and evidence provided by the testers. This ensures that the test meets all set requirements and standards, and that the findings match reality. This ensures the reliability of the study because it shows that the pen test was performed by qualified professionals, that all required tests were completed, and that the findings were correctly scaled and supported by evidence. This allows an organization to demonstrate that it is "in control" of its security, which not only meets legal obligations, but also increases confidence in the security of its systems.

The broader picture

Brenno de Winter

There are several types of security surveys that organizations can conduct to protect their systems, networks and applications from threats. Each of these methods has a specific focus and provides valuable insights into weaknesses and vulnerabilities within a security infrastructure. The following are common security surveys:

First *vulnerability scanning* is an automated process that scans a system or network for known security vulnerabilities. The goal is to identify and map potential vulnerabilities, such as outdated software, weak configurations or unpatched systems....

The vulnerability scanner uses databases of known vulnerabilities (such as the CVE list) and compares them to the installed software and configurations on a network or system. The scanner generates a report with a list of discovered vulnerabilities.

Advantages: This type of survey is simple, quick and can be performed regularly to maintain a continuous record of vulnerabilities.

Disadvantages: However, it does not provide deep insight into how these vulnerabilities can be exploited and lacks context about the impact of a vulnerability within a specific organization.

The second and core of this book *pentesting* or *penetration testing* is a more in-depth and hands-on approach where hackers attempt to actually break into a system. The goal is to discover if vulnerabilities can be exploited and to simulate how a real attacker would proceed.

A pen test goes beyond a vulnerability scan by actually executing the attack and proving that a vulnerability can be exploited. This provides concrete and actionable security insights.

A third examination, code review, is an in-depth analysis of an application's source code to identify security flaws and logical vulnerabilities. This process can be done manually by experienced developers or security experts, or by using automated tools that search the code for known vulnerabilities.

Because the code is checked directly, vulnerabilities can be detected early before the application goes into production. It ensures that security problems are discovered even before they can be exploited.

Finally, *red teaming* is the most comprehensive and advanced security research, where a team (the red team) simulates the entire attack chain. This research goes beyond individual vulnerabilities or systems. It attempts to test the security of the organization, including physical security, social engineering and business processes.

Red teaming provides a realistic view of how well the entire security of an organization is functioning. It examines not only

technical vulnerabilities, but also weaknesses in people and processes.

Each type of security research has its own focus and offers specific insights. Vulnerability scanning is ideal for routine detection of known vulnerabilities, while pentesting goes deeper into actual attack scenarios. Code reviews are essential for finding vulnerabilities in application source code, and red teaming offers the most comprehensive approach by testing an organization's entire security infrastructure, including human and physical security layers. By combining these studies, an organization can develop a robust security program that focuses on both prevention and detection of attacks.

The methodology

Brenno de Winter

The methodology sounds complicated. The diagram looks intimidating. But all is not so bad. Instead, our goal is to make procuring, performing and reviewing pen testing simpler and more straightforward. What we created, in the end, was an Excel sheet. Yes, okay, it was a lot of work, but once it's created, it's also finished for everyone. The Miaw diagram provides an organized way to show the requirements, outcomes and validation of penetration testing. This schema is designed to clarify what is required within a study, what these requirements provide, what you are missing if these requirements are not met, and how an auditor can test compliance. In addition, for each requirement, the schema includes a relevant procurement requirement that organizations can use to ensure that the study meets the stated criteria.

How the Miaw scheme works

Requirement and Description: The schedule begins with a clear listing of the requirements for an information security examination. These requirements can range from capturing digital reporting to listing mandatory certifications of the investigators. For each requirement, a description is provided that clarifies the context of the requirement. For example, the name of the reporter must be included in the report, which helps make responsibility clear.

Validation: This part of the schema describes how the requirement can be validated by an auditor. For example, if

there is a requirement that the reporter must have a valid certification, the determination is: Is that certification there? Is there evidence of it? This provides guidance for auditors to determine that each requirement is colored with evidence.

What it delivers: For each requirement, what meeting the requirement delivers is described. This can range from providing a higher level of assurance to establishing the responsibility of the individuals involved. Making these benefits clear emphasizes the importance of meeting the requirements.

What to miss in absence: This section describes what is lost if a requirement is not met. For example, the absence of certain information may lead to uncertainty about investigator certification or responsibility within the study. This makes it clear to organizations what the risks are if not all requirements are followed.

Procurement requirements: Each requirement is associated with a procurement requirement, meaning that organizations can specifically require that these requirements be met when procuring penetration tests. This ensures that the right agreements are made and that there are no misunderstandings about what is expected of the penetration testers and the reporting.

And that's all it is. We have not reinvented the wheel but gathered together what was already available and put it into a logical framework. You will recognize much in the requirements from the problems outlined earlier, and if you already have more experience with pen testing, it is a much more familiar material.

What we created

With this scheme, we have created a robust framework that ensures penetration testing is not only performed in a technically correct manner, but also in a way that adds audit value. Through this structured approach, organizations can demonstrate that their security is under control and auditors can easily verify that the testing meets all requirements. This process makes penetration testing more transparent, reproducible and effective in ensuring the security of systems.

The CCV pentest seal of approval.

The Netherlands has a vibrant information security industry. Between companies, the CCV seal of approval for pentesting has been in place for several years. We were asked if these schemes do not clash. Dirk Meij writes the answer, which we fully endorse. - Brenno de Winter

Dirk Meij

From the branch organization Cyberveilig Nederland, the work group Quality and Transparency took the initiative for the CCV Pentest certification. Because the working group's goal is to make it easier to choose between cybersecurity vendors, a number of initiatives have been taken to facilitate this. One example here is the cybersecurity dictionary, which attempts to establish, explain and use unambiguous jargon so that everyone, public and private, supplier and customer, speaks the same language. Another initiative is a number of certifications monitored by the CCV of which CCV Pentest is one.

The reason for creating the CCV pen test is to have suppliers meet a minimum set of requirements. This way, a potential customer can pick up multiple quotes and compare them without fear of an improper pen test. This allows vendors to improve their internal processes to meet the minimum requirements. These requirements include minimum reporting content, how a pen test is performed and minimum training requirements for a pen tester. Of course, vendors are free to provide additional services.

As mentioned above, the buyer can request a number of quotes from different pen test suppliers. The certified ones are listed in the register of the CCV on its website. Basically, the quotes are all for the same product and quality as prescribed. This allows the potential buyer to focus more on other things that are more important to him, such as for example a "click" between the buyer and the supplier, but above all on the price. Comparing bids is thus greatly simplified and the guarantee of quality is guaranteed.

The major advantage of the CCV pentest seal of approval is that everyone will do basically the same job, with reporting that is standardized. The advantage of this is, first, that reports can be compared to each other, should differently pen tests be performed by different parties over time. Another advantage is that vendor A's reporting can be valued by vendor B, should a discussion arise.

The downside of CCV Pentest seal is that critics cry that it is a "butcher inspecting his own meat," a "certificate for and by cybersecurity companies. This is indeed the case, but so far it is the only certificate with a quality requirement established by a number of self-critical companies whereas much transparency as possible has been applied. The end goal, providing a pentest of high quality, has been achieved though, and that is the most important thing.

Miaw's initiative is an extension of the CCV pentest mark and not a threat. It can only lead to a better quality of pen testing and pen testing suppliers that ultimately benefits the customer. The CCV certification provides a minimum set of requirements allowing a trade-off between suppliers with the guarantee of content equivalent product and the Miaw gives suppliers visibility on quality delivery. The combination provides a basis for further expansion and improvement of the product pentesting and we challenge everyone to contribute to this.

Process of a pentest investigation

Mischa van Geelen

Why processes are so important

The process surrounding pen testing plays a crucial role in the effectiveness of security research. Following structured methodologies and processes can minimize the risk of errors and ensure that all important aspects of the IT infrastructure are thoroughly examined. A systematic approach ensures that nothing is overlooked and that the results are reliable and reproducible.

A well-structured, planned and executed pentest investigation helps with:

- Identify (critical) vulnerabilities and risks: Through systematic testing, hidden vulnerabilities in systems, applications and networks can be discovered so that timely measures can be taken to mitigate them.
- Improve IT infrastructure security: Understanding the current security status enables organizations to make targeted improvements and strengthen their defenses against cyberattacks.

The role of Miaw and open standards

The Methodology for Information Security Testing with Audit Value provides a structured framework for planning, conducting and reporting pen tests.

Applying this methodology ensures that pen tests are comprehensive, efficiently conducted and provide valuable results that can be directly used to improve security.

Instead of reinventing the wheel, Miaw uses proven, effective and open-source standards for the content execution of pen testing. Some of these standards include:

- Web Application Security Testing Guide (WSTG) - owasp.org
- Mobile Application Security Testing Guide (MASTG) - owasp.org
- IoT Security Testing Guide (ISTG) - owasp.org
- Penetration Testing Execution Standard (PTES) - ptes.org
- Common Vulnerability Scoring System (CVSS) - first.org

Integrating these open standards not only increases the quality of the pen testing process but also ensures consistency and transparency in findings and reports.

As an experienced pentester with more than 100 pentests performed, I know that following structured processes is essential for successful results.

It allows us to proceed systematically, improve customer communication and ultimately contribute to a more secure digital environment. Without a solid process, critical vulnerabilities can be overlooked, leading to serious security incidents.

By recognizing the importance of processes and implementing methodologies such as Miaw, organizations can significantly strengthen their security posture and be better prepared for ever-evolving threats.

Consequences of lack of standards

Ignoring structured methodologies and standards in pentesting can have serious consequences for organizations. As an incident responder, I have experienced firsthand how things can go wrong when a pentester does not fully perform their job due to the lack of a standardized approach. This can lead to incomplete testing, causing critical vulnerabilities to be overlooked.

When pentesters work without a clear methodology, chances are they will not discover all potential security vulnerabilities. This can have very undesirable consequences for the organization commissioning the pen test. At worst, it can lead to enormous damage, such as in a successful hack where sensitive data is stolen, or systems are taken down. The financial impact and reputational damage can be significant, and recovery can take a lot of time and resources.

In certain situations, I was able to demonstrate that if the pen test had been performed according to a recognized methodology, the access paths and vulnerabilities exploited by hackers could and should have been identified. In these cases, the lack of a structured approach directly contributed to the success of the cyber-attack. This highlights the critical importance of following standardized processes in pentesting.

To ensure that pen tests are efficient and effective, it is essential to follow processes described in Miaw. This methodology provides a solid framework that helps systematically identify vulnerabilities. By applying Miaw,

pentesters can perform a complete and thorough evaluation, examining all relevant aspects of security.

Following a standardized methodology also ensures that results are consistent and reproducible. This is important for both internal and external audits. In addition, it increases the credibility of the pen test and stakeholders' confidence in the findings and recommendations.

The benefits of process tracking

Using structured processes in pentesting offers several advantages:

- Structured and standardized approach and reports: This ensures consistency in implementation and documentation, making results easier to understand and compare.
- Increased likelihood of successful pen testing: A systematic approach increases the chances that all critical vulnerabilities will be discovered and addressed.
- Minimizing errors and risks: Following proven methodologies reduces human error and minimizes the chance of overlooking key weaknesses.
- Reduce financial losses from security incidents: timely identification and mitigation of vulnerabilities prevent potentially costly security incidents.
- Auditability for both clients and contractors: Standardized processes make it easier to demonstrate that the pen test was performed thoroughly and according to proper procedures, which is important for compliance and certification.

By embracing these processes, both pentesters and organizations can contribute to a more secure digital environment and strengthen stakeholder trust.

Course of a pen test

In this section, we discuss the various phases that go through during a pen test, based on proven methodologies and standards.

The following chapters will detail each of the six phases:

1. Intake: The initial conversation in which objectives and scope are established.
2. Pre-engagement: Preparing the Plan of Action and formal agreements.
3. Agreement: reaching formal agreement and scheduling the test.
4. Implementation: the actual execution of the pen test according to the agreed methodology.
5. Completion: compiling the report and quality control checks.
6. Third-party validation (optional): The optional external review of the performed pen test.

Below, I will discuss each of these phases and their importance within the pen testing process.

Intake

During the intake phase, the foundation for a successful pen test is laid. During this phase, there is an extensive conversation between the pen testing team and the client. Sample questions that a client might ask can be found at the back of the booklet, in the "Sample Questions" section.

Before you can begin the intake, it is wise to already have a confidentiality agreement in place. This is because information will be exchanged that may be confidential. Some pentesters will already have their first suspicions of findings at the interview.

The goal is to clarify the client's needs and expectations. This involves discussing the objectives of the pen test: what does the client want to achieve, what specific concerns are there, and what results are expected?

In addition, during this phase, the scope of the pen test is roughly estimated. This means that a preliminary list of the systems, applications and networks to be tested is drawn up. Any constraints, such as time, budget or technical limitations, are also discussed. It is essential to get all parties involved on the same page to avoid misunderstandings in later phases.

Finally, attention is paid to logistical and organizational aspects. Consider communication channels, contact people and any necessary means of access. Addressing these issues at an early stage paves the way for the smooth progress of the project.

Pre-engagement

In the pre-engagement phase, the information from the intake is transformed into concrete plans and agreements. A detailed Plan of Action (PoA) is created that describes the methodology, scope, timelines and required resources. This plan serves as the blueprint for the pen test and provides transparency to the client.

In addition, a quote has been prepared that covers the financial aspects of the project. This specifies costs for the various components of the pen test. The scope is formally confirmed to ensure that both parties know exactly what will be tested and under what conditions.

Important legal documents such as safeguard statements are prepared and offered at this stage. These documents protect both the client and the pen testing team and ensure confidential handling of sensitive information. All processes and methodologies used are based on open standards such as OWASP MSTG, ISTG, WSTG and PTES, contributing to a quality and consistent approach.

Agreement

After the client reviews the quotation and the Plan of Action, formal agreement is reached. This involves signing and returning all documentation, including legal agreements. This formal approval is essential to proceed with the planning and execution of the pen test. For a pen test to be successful, it is also important for the client to validate at this stage that the scope objects are correct and complete.

With the signed documents in place, the pen testing team can begin to create a detailed schedule. This includes setting specific dates and times for testing activities, assigning team members and arranging any necessary access to systems and locations.

Moreover, at this stage, all stakeholders involved are informed about the upcoming activities. This ensures transparency and allows everyone to prepare for their role in the process. Confirming agreement lays the foundation for a structured and efficient execution of the pen test.

Implementation

Execution is the core phase of the pentest process in which the actual testing takes place. The pentest team performs the tests as described in the Plan of Action and the bid, with strict adherence to the agreed scope and methodologies. This involves using both automated tools and manual techniques to identify vulnerabilities and security flaws.

During testing, the steps taken, the systems tested, and the findings are carefully documented. This is crucial for transparency and for being able to reproduce results. Any scope objects that are inaccessible or cannot be tested are documented in detail and reported to the customer so that action can be taken on them.

Upon completion of the testing activities, a comprehensive report is prepared. This report is based on open standards and contains a summary of all findings, including risk assessments and recommendations for mitigation. The goal is to provide the client with a clear and actionable understanding of the security status of their systems.

Completion

In the finalization phase, the report is further refined and prepared for presentation to the client. The report undergoes a thorough peer review within the pentest team to ensure accuracy, completeness and quality. Feedback from this review is incorporated to optimize the final result.

All evidence materials collected, such as log files, screenshots and proof of concepts, are organized and securely stored. These materials support the findings in the report and may be important for any follow-up actions or audits.

In addition, all checklists and documentation used are checked and ticked off. This serves as internal quality control to ensure that all planned testing activities have been performed and that nothing has been overlooked. This prepares the pentest team for the final presentation and any questions from the client.

Third-party validation (optional)

In some cases, the customer or an external party may need additional assurance about the quality and results of the pen test. In this optional phase, an independent validation is performed by a third party, such as an auditor.

The third party reviews the evidence, methodologies and reports provided. Based on this, a litigation report is issued confirming that the pen test was performed according to proper procedures and standards. This can be of particular interest to organizations that must comply with specific regulatory or industry standards.

This extra step not only provides greater confidence in the results, but it can also contribute to the organization's information security reputation. It demonstrates a willingness to be transparent and thorough in securing systems and data.

The standards from the methodology

Brenno de Winter

There are several standards, which play a role in performing pen testing. For performing tests, there are publicly available testing guides and testing schemas available from the Open Web Application Security Project. This way, you know exactly what is eligible for testing in each case. As a result, you won't forget to perform basic checks.

OWASP offers several test guides focused on security testing for specific types of applications and technologies. The following are a few key OWASP testing guides.

OWASP Web Security Testing Guide (WSTG).

The OWASP Web Security Testing Guide is a comprehensive guide to Web application testing. It provides a systematic approach to assessing Web application security and covers several test categories, including information gathering, configuration management, authentication, authorization, session management, input validation and more. The WSTG is suitable for pen testers, developers and security professionals who want to assess Web application security. It provides detailed techniques and test cases to detect different types of vulnerabilities.

OWASP Mobile Security Testing Guide (MSTG).

This guide focuses specifically on mobile application testing. The MSTG provides guidelines for identifying and analyzing security issues in mobile apps, with specific focus on both iOS and Android platforms. It includes tests for app security, data storage, network communications, and platform-specific threats. The MSTG is suitable for security professionals and developers focused on mobile application security. It provides methodologies for testing vulnerabilities such as insecure data storage, weak encryption, and insecure network connections.

OWASP API Security Testing Guide

This guide focuses specifically on testing Application Programming Interfaces (APIs). It provides a detailed approach for identifying security issues specific to APIs, such as authentication and authorization issues, insecure configurations, and data processing vulnerabilities. This guide is useful for pen testers and developers who want to ensure the security of APIs. The guide helps detect vulnerabilities such as insecure endpoints, inadequate access control, and misconfigurations.

OWASP IoT Security Testing Guide

This guide provides guidelines for testing the security of Internet of Things (IoT) devices and their ecosystems. It includes methodologies for testing various aspects of IoT, such as device firmware, network communications, hardware interfaces, and cloud backend security. Suitable for security professionals focusing on IoT security. It helps identify vulnerabilities such as weak passwords, insecure firmware updates, and unencrypted communications.

All guides provide a structured approach to assessing different types of applications and technologies. They help identify and address specific vulnerabilities and contribute to a better security posture of software and systems.

You often see pentesting still referred to the OWASP TOP-10 for pentesting. Only this list does not include testing and sometimes even things you cannot technically test for but should audit for.

The OWASP Top 10 is primarily intended for educational purposes and focuses on raising awareness about the most common security risks in Web applications. It provides an overview of common vulnerabilities, such as SQL injection or insufficient logging, and is useful to help developers and security professionals improve their knowledge about security. However, the OWASP Top 10 is not a comprehensive standard or testing framework for a penetration test. It contains only a set of guidelines and examples of vulnerabilities that are widely encountered, but it is not suitable as an in-depth auditing or validation tool.

A penetration test requires much more than just checking the OWASP Top 10. It is an in-depth process that focuses on both technical and context-specific risks, depending on the infrastructure, business and application. For example, a good example of something that is not easily tested against the OWASP Top 10 is business logic flaws. These are vulnerabilities in how the application implements business rules and how those rules can be exploited by attackers. Business logic vulnerabilities require in-depth knowledge of the application context and cannot be detected by generic checking against the OWASP Top 10.

Another concrete example of what is not easily covered by the OWASP Top 10 is testing a complex multifactor authentication system specific to a customer's enterprise environment. A vulnerability where the authentication mechanism can be bypassed through a combination of session takeover and timing attacks requires specialized penetration testing scenarios beyond the known OWASP vulnerabilities because it requires specific technical configurations and business conditions to understand where the problem lies.

Sometimes people still refer to the OWASP Application Security Verification Standard (ASVS). However, this useful standard is not suitable for performing pen testing because it is designed primarily as a framework for assessing the security requirements of Web applications and not as a hands-on testing methodology. ASVS focuses on defining security controls to be implemented in the software development cycle and provides a detailed list of verification requirements for developers to follow. It does not specify techniques or procedures for actually testing vulnerabilities in an application, as pen testing does. It is important to realize, however, that for a *code review* ASVS is very useful!

Pentests focus on identifying real security problems in an application through active attacks and exploitation of vulnerabilities. In contrast, ASVS offers a checklist approach more suited to audits and assessing the completeness of security measures, without the in-depth hands-on attacks typical of a penetration test.

Standard for severity of findings: CVSS

Scoring vulnerabilities is an essential part of any security process, and the Common Vulnerability Scoring System (CVSS) provides a standardized approach for doing so. CVSS helps security professionals assign vulnerabilities a score ranging from 0.0 (informational) to 10.0 (critical), which determines the importance and priority of vulnerabilities. These scores numerically represent the severity of a vulnerability and are based on a combination of three main parts: the Basic Score, the Temporal Score and the Environmental Score. Each of these parts provides valuable insights that help manage security risks.

Starting point: The basic score

The first step in grading a vulnerability is to calculate the baseline score. This part of CVSS focuses on the intrinsic properties of the vulnerability that remain immutable regardless of time or specific circumstances. The base score assesses the vulnerability in two areas: exploitability (how much abuse you can take of it) and impact (what are the consequences).

Exploitability considers factors such as how the vulnerability can be accessed (via network access or locally), the complexity of the attack and whether user interaction is required. This gives an idea of how easy it is for an attacker to exploit the vulnerability.

The impact is then assessed on three core aspects of information security: confidentiality, integrity and availability.

Will sensitive data be exposed? Can an attacker modify or delete data? Does vulnerability affect service or system availability? Each of these questions plays a role in determining the base score, which ranges from 0.0 to 10.0, with higher scores indicating more serious vulnerabilities.

Time score: variable conditions

After the baseline score is established, the temporal score comes into view. This takes into account the dynamic factors that affect exploitation of vulnerability. Consider the availability of exploit code that facilitates abuse of the vulnerability, or the availability of a patch or workaround that can mitigate the impact.

The temporary score adds a layer of flexibility to the model, allowing vulnerabilities to be scaled based on current information. For example, if a patch is available, the temporary score can be lowered to account for the reduced threat. This helps security professionals respond to changing conditions and better prioritize vulnerabilities as more information becomes available.

Environment score: the context

The environment score adds a third dimension to the model by taking into account the specific context of the organization. Instead of scaling vulnerabilities based solely on their technical characteristics, the environment score takes into account

factors such as the value of the affected system, the sensitivity of data and the extent to which a vulnerability can actually be exploited in the given situation.

With version 4.0, CVSS has paid more attention to adding contextual data. This means that during the intake of a pen test, detailed information is gathered about how and where the vulnerabilities might impact the organization. How important is the affected system to business operations? What is the data that needs to be protected? Are there additional security measures in place that could mitigate the impact? These questions help evaluate the findings not only from a technical perspective, but also from a business risk perspective.

Classification

Scaling vulnerabilities with CVSS involves a number of steps. It starts with the Basic Score, which assesses the inherent properties of the vulnerability. Then the Temporary Score is adjusted based on factors, such as is exploiting code available and what can you do to mitigate the impact or is a fix already available? Finally, the Environment Score is applied to refine the score based on specific organizational context. The end result is a score indicating how serious a vulnerability is, broken down into the following categories:

1. 0.0 - Informational: Vulnerabilities with a score of 0.0 do not pose a direct security risk but can provide useful information for improvements. For example, consider

configuration warnings or information that does not pose a direct threat but deserves attention.

2. 0.1 to 3.9 - Low: These vulnerabilities have limited impact and are difficult to exploit. They do not pose an immediate security threat but may require attention over time to minimize potential risks.
3. 4.0 to 6.9 - Medium: Findings in this range are real and have significant impact. They are not always easy to exploit but can still have significant security implications under specific circumstances. Addressing these vulnerabilities is important to prevent escalation of risks.
4. 7.0 to 8.9 - High: These vulnerabilities pose a significant risk and can be easily exploited. They significantly impact the confidentiality, integrity or availability of systems. Action is required to resolve these issues quickly.
5. 9.0 to 10.0 - Critical: Vulnerabilities with a score in this range pose a serious threat. They are often easy to exploit and can lead to complete compromise of systems or data. Immediate action is necessary to prevent damage.

The intake is important for scoring

With a well-thought-out approach to pentest intake - in which the context of the business environment is clearly understood - CVSS scores can be used effectively to create action plans and optimize security resources. By looking not only at the technical details but also at the business impact, risk management is aligned with the real needs of the organization.

Through this structured approach, CVSS provides not only a numerical value for vulnerabilities, but also a holistic understanding of the threats that can actually affect the organization. This makes it an indispensable tool for managing cybersecurity risks and prioritizing remediation actions.

The eternal exception: CIS controls

Among the lists of checks to perform are the CIS checks, a set of information security guidelines developed by the Center for Internet Security. They are designed to help organizations improve their security by offering practical measures that reduce the likelihood of security incidents. These controls focus on best practices such as inventorying hardware, managing software updates and setting access rights. While they provide a useful framework, failure to meet a specific control does not automatically mean that a system is vulnerable; rather, it may indicate increased risk.

One of the biggest causes of security incidents is configuration errors. These errors occur when systems, networks or applications are not set up correctly, causing security breaches. Examples include poorly configured firewalls, databases with unrestricted access or the use of default passwords. Research shows that 80% of security incidents are related to improper configurations. This underscores how important it is to manage configurations properly and regularly check for errors.

Configurations play a crucial role in security because they determine the access and functionality of systems. A properly set configuration can mitigate potential threats, while an incorrect configuration creates opportunities for attackers. Configuration errors can occur in virtually any environment, and often they are the result of human error, lack of knowledge or inadequate oversight.

CIS controls help identify and prevent configuration errors by providing clear guidelines on how systems should be set up and managed. For example, they describe how firewall settings can be optimized, what minimum access rights are required, and how logging and monitoring can be effectively applied. This enables early detection and correction of configuration errors.

Failure to comply with a CIS control does not directly mean that an organization is vulnerable to attack. Controls are intended as guidelines to reduce risk and improve overall security posture. Failure to comply with a control may indicate a potential weakness, but it does not necessarily mean that a system can be immediately exploited. In addition, there are controls that are simply so general that they are not applicable. Take a mail server, for example. Based on the CIS controls, the mail server will be a finding. But for the purpose (mail server), that is a logical finding that it is encountered. Similarly, failure to follow a hardening control may be necessary for a service to run at all.

The context in which a configuration error occurs plays an important role. For example, an incorrect configuration on a public server can be much more dangerous than the same error on an internal system with no external access. This makes clear

why configuration errors cannot be automatically assigned a CVSS (Common Vulnerability Scoring System) score. CVSS is designed to rate vulnerabilities in software code based on their exploitability and impact, whereas configuration errors are more dependent on environmental factors and the specific use of a system. Therefore, the report only indicates it as found or not found without value judgment. The explanation of the party being investigated is the input for the recipient of the investigation. After all, the latter must be in control.

Configurations are essential to system security and play a major role in preventing security incidents. CIS controls provide a useful framework for preventing and correcting configuration errors, but non-compliance with a specific control does not automatically indicate a direct vulnerability. Understanding that configuration errors cause 80% of incidents further emphasizes the importance of proper management and control of configurations. Complying with CIS controls helps create robust security, minimizing risk and increasing resilience to attacks. But not complying is not automatically wrong. A CIS finding is nothing more than a determination that a rule has not been followed without being able to directly attach a value judgment to it. These get no more in the report than a finding without a CIS score.

The report

Brenno de Winter

With Miauw's schedule comes a pen report template. It was created by Jeroen Diel, Mischa van Geelen, Maaike Hielkema and me. This template was developed to provide pentesters with a clear and professional structure for recording their research and findings. All points from the methodology have been incorporated into the report. This also makes the report itself a tool that nothing is forgotten.

This format helps ensure consistency in reports and ensures that all key elements are systematically documented. The report begins with a document management section that lists basic project information, such as client name, project reference and confidentiality classification according to the Traffic Light Protocol (TLP). This makes it clear from the start who has access to the report and how the content is to be protected. In addition, the template provides a detailed overview of version management, so that involved parties can always retrieve what changes have been made and by whom.

The author's accreditations section plays an important role in enhancing the credibility of the report. Listing relevant certifications and qualifications of the pentester, such as OSCP or OSEP, along with supporting documents, demonstrates that the findings were prepared by a qualified professional. By then providing a signature, the professional attests to having performed the investigation to the best of his or her knowledge and belief. Combined with the extensive version history, this provides transparency and gives insight into the evolution of the report and the steps taken.

The Miaw concept template is designed primarily to help pentesters get started, by giving them clear guidelines for preparing a professional pentest report. This low-threshold approach enables anyone, from beginners to experienced professionals, to write a high-quality report that meets the professional standards of the field. In this way, the accessibility of pen testing is increased so that more people can contribute to improving security.

In addition, the template is valuable for auditors. After all, under the methodology, they issue a case report. This is because the format of the report allows the findings to be used directly as a basis for further legal documentation. Based on the carefully documented findings and analyses, an auditor can issue an official report that meets the requirements for formal reports. This makes the draft report not only a tool for pentesters, but also an essential component in the audit and legal follow-up process, thus increasing the quality and reliability of the entire security chain.

The record

Brenno de Winter

After performing an information security examination with audit value, an auditor can prepare a process report based on the Miaw diagram. In this process, the auditor does not re-run the investigation but does check for each requirement to ensure that sufficient evidence has been gathered. This creates a clear overview of what was or was not documented during the penetration test. It is then clear to the recipient what parts of the object were examined in the penetration test, what findings were recorded, and whether or not there is "in control" based on this information.

The process report adds significant value by increasing the independence of the investigation. The auditor involved is an outside party who objectively reviews the work of the pen tester. This ensures that an additional layer of control is added, giving the organization greater assurance that the investigation was conducted thoroughly and according to proper procedures. This objective determination reinforces confidence in the findings and ensures that there are no one-sided interpretations or missed areas of concern.

In addition, the record provides valuable insights for management, who often have less technical knowledge. By presenting the findings in a clear and structured way, they can better understand what the results mean. This helps in making informed decisions about which risks prioritizing and what actions to take. The litigation report allows management to gain

insight into the level of compliance and security without having to dive deep into the technical details.

Being "in control" means that an organization has taken sufficient measures to manage risks and comply with relevant laws and regulations. This is critical for legislation such as the General Data Protection Regulation (AVG), which requires organizations to take appropriate technical and organizational measures to protect personal data. It also applies to the Financial Supervision Act (Wwft) for financial institutions that must have their information security in order and the NIS2 Directive (Network and Information Security Directive), which provides for higher requirements for cyber security in sectors with critical infrastructure. In the Netherlands, this is implemented in the Cyber Security Act. The official report may also be relevant for ISO 27001 or NEN7510 certification, where there are strict requirements for compliance with information security standards. In all these cases, the investigation is reproducible and actually tested.

Litigation helps organizations demonstrate compliance with these laws and regulations by providing insight into which security measures are effective and where improvements are still needed. This not only increases compliance with the law but also strengthens resilience against security incidents and data breaches, helping to manage legal and financial risks. In short, the official report is an essential part of the audit process that not only ensures the objectivity and thoroughness of an investigation but also helps ensure compliance with important

laws and regulations, thus contributing to the overall control and resilience of the organization.

Legal aspects of pen testing for clients

Victor de Pous

Core message

A penetration test (pen test) is an essential form of digital security research, as it can proactively identify vulnerabilities in network and information systems before (un)intentionally caused incidents occur. Reactively, the pentest proves its value, among other things, in identifying the cause, assessing the extent of damage and implementing corrective measures to prevent recurrence. Knowledge of the various legal aspects of pen testing is a basic prerequisite for each client's lawful and effective execution.

Principles

1. Information security is a legal obligation (duty of care) for every organization in the Netherlands. Central government organizations must also implement policy rules concerning information security, as laid down in the Government Departments Information Security Regulations Decree 2007, the Government Departments Special Information Regulations Decree and the Government Information Security Baseline (BIO).

2. Part of this legal duty of care is verifying that the risk management measures in place are implemented, complied with and remain adequate on an ongoing basis. Accountability in this regard has also become increasingly important due to

transparency and reporting requirements. These and other processes, such as incident response, require the execution of digital security research.

3. The penetration test is an important form of security research, which is an integral part of a coherent information security policy and is generally considered indispensable for strengthening digital resilience. VWS Concern uses the following working definition:

> *"An offensive security investigation to be conducted by one's own personnel or third parties, which involves a controlled search for vulnerabilities in one or more secure network and information systems or components thereof, which could be used to break into these systems and/or which, without intention or autonomy, could disrupt or otherwise adversely affect the data processing of the organization under investigation."*

4. Performing a pen test requires diligence. Factually (technically and operationally), a pen test focuses on identifying as many vulnerabilities as possible without causing damage to network and information systems. Legal due diligence is essential in the design, planning and execution of offensive operations, which means strict compliance with applicable legal and policy frameworks and precise adherence to the assignment (contractually defined when outsourcing).

5. In addition, it is important that the findings of a pen test be traceable, verifiable and evidentiary of sufficient weight (audit value). The results should be reproducible, verifiable, clear, accurate and provided with context and recommendations for mitigation. Following industry norms and standards contributes to consistency and reliability.

Introduction to legal aspects

Information security ("information security") refers to securing computer systems, networks and data on the basis of risk mitigation and management. It is the set of technical, organizational and operational measures that focuses on the continuous assurance of the confidentiality (where only authorized users have access to the systems and data), integrity (where processed data is complete and accurate), and availability (where users have access to systems when needed).

The broad societal importance of information security stems from the protection of fundamental rights, national security, continuity of services, economic stability and trust in the digital society. Consequently, information security is a multidisciplinary field in which technical, organizational and legal expertise are integrated and work together seamlessly.

However, digital systems can contain errors and other imperfections that autonomously and unintentionally weaken the security and proper functioning of the system, network or its components, such as computer programs or protocols. This is increasingly being exploited by criminals and state actors.

In fact, and in law, vulnerabilities are primarily referred to in this context. Following the EU Regulation Cybersecurity Act (CSA), the revised EU Network and Information Systems Security Directive (NIS2), which will also apply to central government organizations on Oct. 18, 2024, understands a *"vulnerability" to* mean "a weakness, susceptibility or deficiency of ICT products or ICT services that can be exploited by a cyberthreat" (Artice 6, para. 15 of the NIS2).

A *"cyber threat,"* according to European law, is "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact t network and information systems, the users of such systems and other persons" (Article 2(8) of the CSA).

Identifying vulnerabilities in ICT systems requires prudent research. An essential form of digital security research is the penetration test (pen test), in which the researcher assumes the role of a malicious actor (attacker) and makes a controlled attempt to penetrate a network, information system or a specific part of it, such as an application.

The outcome of the pen test must lead to the identification of one or more traceable, verifiable and reproducible findings, which are in principle confidential. The pentester then reports these findings to the internal or external client, with a detailed analysis, description and classification of the vulnerabilities, supplemented by solution-oriented advice to strengthen the digital resilience of the organization under investigation.

This memorandum briefly discusses some of the legal aspects of pen testing. This is necessary because the law plays an important and dual role in conducting these offensive digital security investigations. Knowledge of the legal aspects of pen testing:

- Supports risk management measures (duty of care) and compliance with other legal, policy and contractual security requirements, including reporting and accountability (*legal compliance*);
- Provides points of attention for conducting security investigations more effectively within the mandatory frameworks (*value creation*).

The second facet may be understudied. By understanding the legal frameworks, both clients and pentesters can not only act lawfully, but also optimize their approach. For pentesters, this means that they can adapt and refine their methodology to achieve maximum results within legal boundaries, leading to more effective and efficient security investigations.

Both facets help strengthen digital resilience, including post-incident recovery capability, and reduce the risk of legal liability of organizations.

Information Security Law

From the perspective of good (public) governance, it is advisable to have at least basic knowledge of the legal framework of ICT, including information security, and access to

specialist knowledge to support it. This principle also follows the NIS2 Directive, which explicitly states that both information security and compliance with this law is a board responsibility. Among other things, individual directors are subject to an education requirement.

Every organization is nowadays obliged to secure ICT, because the legal non-committal nature of taking protective measures is behind us. For example, this obligation has applied to the holder of a personal data record since the phased entry into force of the first Dutch privacy law, the Personal Data Records Act, which went into effect on July 1, 1989.

Information security is currently being increasingly prescribed in laws and regulations, especially by the European Union. That process began with the 1995 Data Protection Directive, which the Netherlands implemented through the Personal Data Protection Act (Wbp) and which went into effect Sept. 1, 2001. In addition, every organization is bound as a contracting party to agreements with a digital security component.

There are also policies specifically for central government organizations. For example, since January 1, 1995, the Central Government Information Security Regulations Decree (VIR 1994) had been in force, while now the 2007 version (VIR 2007) applies. Incidentally, security regulations in relation to computer systems and data processing were already in force for the central government at the beginning of the 1980s .[1]

It is worth remembering that the legal aspects of information security are broader than typical single-issue legislation or policies, such as the NIS and NIS2 Directives and the Government Information Security Baseline (BIO).

Indeed, while information security focuses on mitigating and controlling risks that can threaten the confidentiality, integrity and availability, of information, the focus of the legal aspects of information security is considerably more extensive.

In addition to legal obligations, the field of law includes definitions, rights and other legal norms, such as rules for liability, prohibitions and supervision and enforcement. Information security law is therefore an integrative subject that horizontally cuts across the traditional, vertical division into state law, private law, criminal law and administrative law.

However, this qualification does not alter the fact that the legal and policy duty of care to secure is a central component. This always involves addressing the overall problem of lack of confidentiality, integrity, and availability, of data processing.

[1] https://autoriteitpersoonsgegevens.nl/nl/nieuws/nieuwe-eu-brede-regels-avg-boetes-bedrijven-op-komst

Legal obligations

Various laws and policies require organizations to implement risk management measures to protect computer systems, networks, their users and others from threats, incidents and their consequences. In principle, this legal duty of care applies to every organization.

The purpose of the measures is to proactively and preventively ensure the confidentiality, integrity, and availability of data (in fact, its processing). Confidentiality includes authentication, identification and authorization, as these concepts are directly related to protecting access to data.

Focusing on all three core concepts is crucial to a balanced approach to information security. That said, protecting each core concept individually is important and a violation of any one of these elements also constitutes a security problem.

In addition, reactive and corrective measures are prescribed to respond quickly and effectively to security incidents, limit damage and take remedial action. In addition to the legal duty of care - mostly, but not exclusively, based on open, risk-based and technology-independent standards and taking into account the state of the art, international standards and, for example, implementation costs - other mandatory regulations apply. One example is reporting obligations, including incident information obligations and a registration requirement for critical and important entities under the NIS2 Directive. Registration helps authorities have an overview of relevant entities and provides a more coordinated approach to information security at the national and EU level.

In addition, transparency and "accountability," which in this perspective means accountability for information security, are becoming increasingly important socially and legally. A crucial part of this accountability is documentation requirements. Organizations must maintain documentation that demonstrates the measures taken to secure information and the enforcement of those measures.

Furthermore, board members of an essential and important entity within the meaning of the NIS2 Directive must undergo training (education obligation), Moreover, personal liability may arise for them if the organization fails to comply with the rules. It follows emphatically that both information security and its legal frameworks have become *Chefsache*. It involves formal, active and substantive involvement.

For example, administrators must have the appropriate knowledge to assess, approve and oversee the risk management measures to be implemented. This is an ongoing process, which includes prescribed education and training, including the legal aspects of information security.

Supervision and sanctions

A hallmark of information security law is government oversight, which serves several purposes. This includes ensuring compliance with laws and regulations, which is important to ensure that organizations implement and monitor required measures. Oversight helps protect society by ensuring the security of critical infrastructures and services that are vital to daily life and the economy.

In addition, government surveillance helps prevent digital threats by identifying, addressing and informing about vulnerabilities and potential risks. Active surveillance and enforcement by government agencies ensure that organizations can respond quickly and appropriately to emerging threats.

Violations of legal security obligations for network and information systems are usually subject to heavy penalties in the form of administrative fines from a regulator. The threat of high administrative fines that must be "effective, proportionate and dissuasive" in nature (e.g. Article 83(1) of the GDPR, Article 34(1) of the NIS2) usually reinforces the importance of legal standard-setting and the need to comply with it by checking for compliance.

The level of administrative fines imposed by a European regulator for violation of privacy laws has now been harmonized. Here, the size of the organization is the starting point, followed by the qualification of the severity of the violation: low, medium and high. What this system will look like under the NIS2 Directive in the Netherlands is not yet known.

A fine imposed by a regulator does not affect the fact that a person harmed by a safety incident can go to the civil courts to claim compensation for attributable damage. Moreover, one can observe an upward trend in Dutch legal practice in class actions pursuant to the Law on the Settlement of Mass Damage in Collective Action (WAMCA).

Investigation as a legal duty of care

Every organization must take security measures for network and information systems. This duty of care involves a clear premise regarding responsibilities. “As indicated in the Dutch Cybersecurity Agenda and the Roadmap Digitally Secure Hardware and Software, organizations are primarily responsible for cybersecurity themselves. Software manufacturers are primarily responsible for the digital security of the products and services they offer,” said the Dutch Minister of Justice and Security in 2022.

From the duty of care stems the obligation to conduct security investigations. On the one hand, this involves checking whether the measures implemented are effective and remain appropriate to current threats. On the other hand, investigation is required as part of incident response, which includes analyzing the causes and consequences of security incidents.

In addition, security investigations are necessary in several other situations. For example, they are crucial after major system changes, such as software updates or system migrations, to ensure that no new vulnerabilities have been introduced. When meeting compliance requirements, pen tests are a mandatory part of security policies.

Further, they should be conducted prior to the implementation of new applications to ensure security, and as part of an ongoing information security program to proactively identify and remediate weaknesses. Finally, digital security investigations

play a role in due diligence (investigation and review process) in mergers, acquisitions, or collaborations, to evaluate digital risks.

The general rule of law in the Netherlands is that everyone should behave in accordance with social care. Violation of this important legal principle by an act can be unlawful under certain conditions (Article 6:162 of the Civel Code). It is not inconceivable that the failure to conduct a digital security investigation, resulting in damage, may be considered unlawful if, in addition to the damage, the other requirements are also met unlawfulness, accountability, causality, and relativity.

Moreover, specific legal requirements apply (directly or indirectly) regarding the conduct of security investigation or are on the agenda:

- A provider of an essential service and a digital service provider are obliged to take 'appropriate and proportionate technical and organizational measures to manage the risks to the security of their network and information systems'. This in any case includes 'supervision, control and testing' (Article 7(1)(d) of the Wbni);
- A data controller and a processor must have " a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing” (Article 32(1)(d) of the GDPR).

- An essential entity and an important entity must implement a measure aimed at " security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure " (Article 21(1)(e) of the NIS2).
- “ The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following: (..): policies and procedures to assess the effectiveness of cybersecurity risk management measures” (Article 21(2)(f) of the NIS2).

In addition to monitoring the implementation and operation of risk management measures, monitoring incidents requires attention and execution. This is also subject to direct legal requirements (Article 7(1)(b) of the Wbni, Article 32(1) of the GDPR and, for example, Article 21(1)(b) of the NIS2). Such an incident may also entail for the affected organization the general legal obligation to prevent or limit damage (according to the doctrine of tort and/or an obligation to limit damage ex contract law).

- As far as known, the EU regulation DORA is currently the only legal framework that explicitly defines a ('threat-led') penetration test. (Article 3(17) of the DORA) and requires certain financial entities to conduct such a test once every three years (Article 26(1) of the DORA). The public sector policy BIO, on the other hand, requires that government organizations audit their

information systems annually "for technical compliance with security standards and risks with respect to actual security. This can be done, for example, by (automated) vulnerability analyses or pen tests (Article 8.8.2 of the BIO). The VNG has prepared a guide for this. In this context, see also the NCSC's white paper Security testing. Also, when using the digital authentication system of the Dutch government DigiD, an annual audit is mandatory in the connection conditions for customers and the audit statement to be sent to the Minister of the Interior and Kingdom Relations.

Accountability under European privacy law, as enshrined in the GDPR affects the conduct of digital security surveys. According to Article 5(2) of the GDPR, the data controller is not only responsible for compliance with the six privacy principles (including security),but must also be able to demonstrate compliance ("accountability" in the form of accountability)By examining regularly, organizations can demonstrate that they are taking proactive measures to ensure information security and meet their obligations. In addition to the privacy legislation (Article. 32(1)(d) of the GDPRAVG), this line is reflected in other standards, such as ISO 27001 (general) and, for example, NEN 7510 (special: for the Dutch healthcare sector). Performing a pen test is a way of demonstrating and proving compliance with security requirements, which is elaborated, for example, in the "controls" of NEN7510 for outsourced software development (Articles A.14.2.7, A.14.2.8 and A.14.2.9).

The Cyber Resilience Act (CRA), whose text was adopted by the European Council on October 10, 2024, introduces new cyber

security obligations for hardware and software products placed on the EU market.

Among other things, the CRA introduces a system of duties of care, i.e. essential risk-based digital safety conditions for all products with digital elements (horizontal) that manufacturers, suppliers and importers (supply chain) of such products must comply with prior to first making them available in the internal market and during the product's life cycle, complemented by market surveillance by public authorities.

Key elements of the CRA include requiring manufacturers to apply security-by-design principles, conducting conformance assessments and timely reporting of vulnerabilities and security incidents. The legislation also imposes responsibilities on importers and distributors to ensure that products meet digital security requirements before they are placed on the market.

Penetration testing

Penetration testing is widely regarded as an essential method of fulfilling the legal duty of care for information security, both proactively and reactively. They help identify vulnerabilities in systems and processes, and in this way contribute to strengthening digital resilience, even after incidents.

A penetration test involves requested and controlled intrusion, or at least attempted intrusion, into network and information systems. Intrusion without authorization also occurs, but by

criminals, state actors and ethical hackers. The latter category acts out of social commitment and without unlawful intent.

Whether pen testing is performed internally or externally, manually or automated, static or dynamic, one-time, periodic or continuous (monitoring), or based on a combination of these, structural testing of one's own organization is considered a best practice and critical component to improve and accelerate the proactive approach to information security. This applies even more to producers and suppliers of digital products and services. After a security incident, a pen test can help reactively identify the cause, assess the damage and identify vulnerabilities that have been exploited. This supports improving security measures and preventing future incidents (incident response and analysis).

As described above, VWS Concern uses the following description of a penetration test as a working definition as a collective term:

> *" An offensive security investigation, conducted by internal personnel or a third party, which involves a controlled search for vulnerabilities in one or more secured network and information systems, or components thereof, that could be exploited to break into these systems and/or unintentionally or autonomously disrupt the data processing of the organization under investigation, or otherwise cause adverse effects”*

The controlled modus operandi means that the investigation process is carefully designed, planned and executed within agreed frameworks to ensure that the system or network does not incur avoidable damage and that the test is carried out lawfully.

Pentests can have a broad focus and focus on general investigations of vulnerabilities, but there is also a specific type of pentest that uses detailed information about specific threats and attacker scenarios. Thanks to EU Regulation DORA, a legal definition is now available for this type of test. A "threat-led penetration test" ("threat-led penetration testing" or TLPT) is defined as:

> *" “A framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity’s critical live production systems " (Art. 3(17) DORA).*

It follows that part of the diversity of pen testing is reflected in the information position of the person conducting the investigation. As the pentester has more inside information and access rights to the system or network being tested, there is more to investigate and experiment with. With that, the scenario also changes. It is important to realize that, as a rule, the stronger the information position, the greater the number of findings.

In its most basic form, there is a "black box" test. Here, only the strictly necessary information is available, such as an IP address or a URL. In a "gray box" test, more information is available, such as details about underlying networks, systems and a user account. A "white box" test involves giving the investigator full access to the system or network, including the source code of computer programs. This can provide a complete security picture. A careful determination and description of the scope of a pen test in a Statement of Work (SoW), including purpose limitation, test period and expiration date, is of great importance to both the researcher and the organization being investigated. Here, breadth (scope: network, server and application level) and depth (system layering and access rights) weigh in. For the pen tester, he needs to know what and how deep to penetrate, while the organization benefits from a good, substantive and most optimal test to verify and improve security. It is important to note, however, that in practice this determination is often incomplete or inadequate. For the client, there is often a lack of clarity about the investigation, while for the pen tester, it is insufficiently determined what the area to be attacked is until various steps of information gathering have been completed. This means that achieving the best possible security audit may require a dynamic mission description.

Non-Disclosure

Confidentiality plays an important role in conducting digital security investigations. This applies both when internal employees are investigating the organization and when the task is outsourced. Firstly, there is confidential detailed information about the network and information systems, and their components, being examined. Secondly, the findings consist of highly sensitive information about vulnerabilities in a system. If this information, especially the findings, falls into the wrong hands, malicious actors could exploit their weaknesses to carry out attacks.

Confidentiality ensures that the results of the pen test are only available to authorized individuals, which in itself is a risk management measure, as the obligation helps to ensure the confidentiality, integrity, and availability of the data processing of the systems being examined and minimizes the risk of digital attacks. Furthermore, confidentiality protects the organization's reputation and prevents potential legal and financial consequences that may result from unauthorized disclosure

When a pen test is conducted internally, the organization under investigation has more control over who has access to the sensitive information collected during the test. This minimizes the risk of information leaks. Internal employees are typically already bound by existing confidentiality protocols and employment contracts, making it easier to ensure that confidentiality is maintained, the organization has direct visibility into the investigation processes, which helps to quickly identify and mitigate information security risks.

With outsourcing, on the other hand, an external party has access to highly sensitive business information, which increases the risk of leakage. Because the information is beyond the direct control of the organization, it is essential to enter into a non-disclosure agreement (NDA) with the external pen tester. This ensures that any discovered vulnerabilities and other confidential information remain protected and not shared with third parties.

However, the organization must rely on the external party to ensure confidentiality, which makes the importance of contractual agreements on confidentiality and, for example, penalties for breach, even more important. In addition, the pen testing service provider must comply with all relevant laws, regulations and policies, and any breach of confidentiality can harm the outsourcer.

That being said, it does not negate the fact that the public results of digital security investigations can have value in the context of transparency, trust, and accountability. By making certain results of digital security research public, organizations can demonstrate that they are proactively identifying and mitigating vulnerabilities.

This strengthens the confidence of customers, stakeholders and society in the security and reliability of their systems, products and services. Moreover, it can serve to demonstrate compliance with regulatory standards and conformity assessments, as required by the EU Regulation AI Act and, for example, the upcoming EU Regulation CRA.

Standards

Pentest service providers may use proprietary methodologies and techniques, while several recognized standards are available. Applying recognized standards has attractive advantages. It ensures a minimum level of security, and the uniformity created by following these standards prevents or at least helps settle discussions and conflicts. Also, the work of an auditor cannot take place without standardization.

The benefits of standardization are broader: Standards ensure the careful definition of the test subject, detailed documentation of findings, and a structured classification of the severity of findings, which can serve as procurement requirements. This may involve a program of requirements (PoR) or part of it.

It is recommended that available, open security testing standards be part of the formal engagement for a penetration test. For example, the Open Web Application Security Project (OWASP) has established a collection of standards that provide detailed answers to the question of what to test.

Useful resources include, among others, the top 10 most common security vulnerabilities, which are also available for application programming interfaces (API). Based on these lists, a penetration test can no longer rely solely on a scan, as they also highlight errors that make it necessary to question the client, for instance, about the available monitoring. Other OWASP standards oversee testing of Web applications (WSTG) and mobile applications (MSTG). Simply querying standards ensures a minimal level and assumes white box or grey box testing. Standards are also available for reporting the findings of an investigation. The Penetration Testing Execution Standard states meticulously how a test can be recorded. Combined with the requirement that the investigation be conducted in such a way that it is reproducible, it is now possible to have a meaningful counter-evaluation performed on (parts of) the investigation if in doubt. This reproducibility is of great importance for legal and compliance purposes. The reliability and repeatability of the test are then crucial.

Next, the Common Vulnerability Scoring System (CVSS) provides a standardized method for classifying and reporting vulnerabilities, rating the severity of a vulnerability on a scale from 0 (informational) to 10 (very severe).

This scoring method considers several factors, such as potential impact of the vulnerability, exploitation complexity and availability of an "exploit" (a piece of software, code or set of commands that exploits a vulnerability or flaw in a system, software or network to perform unwanted or unauthorized actions).

In addition, the CVSS score can be customized to an organization's specific context, providing a context-specific representation of risk. This allows organizations to evaluate vulnerabilities not only at the technical level, but also in the context of business continuity and operational impact.

Many organizations use a CVSS score of 4 or higher as a threshold, with such a score being considered a blocker for the go-live of new or modified information systems. In this context, the CVSS score acts as an objective risk measure that supports organizations in establishing their risk appetite and tolerance. Since each organization has unique risk profiles and security requirements, they can define additional thresholds depending on their own risk management strategies and security policies. This leads to a more personalized and tailored approach to vulnerability management.

While confidentiality of pentest findings is not in question from a digital resilience standpoint, it may be a strategic choice for clients to share findings with stakeholders after a successful (re)test.

This contributes to increased transparency and strengthens confidence in the organization's implemented security measures. In addition, disclosure can help meet external compliance and certification requirements, such as ISO 27001, which further strengthens the organization's security posture and demonstrates compliance with industry standards.

Pentest as a contractual condition

If a supplier is contractually obligated to secure its client's data processing, this duty of care arising from the GDPR and NIS2 Directive must be contractually secured. This means that the supplier must not only implement appropriate measures, but also actively monitor whether these measures are and remain

effective, through digital security research. These obligations must be clearly defined in the contracts to ensure compliance and address liability in case of non-compliance.

Increasingly, however, the obligation to conduct digital security investigations, including risk assessments such as a DPIA, is being included in agreements even where legislation does not require it. This development reflects a growing trend to proactively comply with higher security standards and mitigate risk.

With the increasing focus on strengthening digital resilience and the search for more quality guarantees and assurances, the user organization can follow the same line with regard to pen testing. In this consequence, a pen test is included as a condition as part of a contract for the delivery of a product or service.

The outcome of a pen test provides insight into the status of information security at a specific time and in a specific case, thus avoiding discussions and conflicts. By recording the findings in a clear and detailed report with audit value, all parties have common ground, which significantly improves cooperation and communication.

Moreover, a code review, DPIA and penetration test can complement each other. A DPIA helps identify and evaluate privacy risks, a code review focuses on detecting errors and security problems in software source code, while a pen test simulates attacks to discover vulnerabilities in network and

information systems. Together, these studies form a holistic approach to information security, covering various aspects.

A pen testing clause then leads to a separate penetration test agreement between the client and the external pen testing service provider. The agreement specifies the scope, objectives, methodology and reporting requirements of the security study, ensuring clear expectations and responsibilities.

These agreements not only improve information security but also promote transparency and trust between parties. In addition, a clear contractual basis contributes to legal certainty and compliance with relevant laws, regulations and policies.

Pentest agreement

The main rule is unmistakable: do not conduct a penetration test without the express consent of an authorized representative of the owner or director of the organization operating the ICT systems under investigation. Without this consent, even the act of merely scanning network and information systems may fall under the offense of computer hacking (Art. 138ab of the Penal Code).

Consent is closely tied to the scope and depth (breadth or "scope") of security research, as defined in a Statement of Work (SoW). In addition to consent, the client typically provides various indemnities to the pen tester. In outsourcing, the arrangements with an external security service provider qualify as a contract for services (Article. 7:400 of the Civil Code).

Based on an indemnification clause included in the contract, a party is indemnified.

In this context, the pentester obtains protection against claims, such as a claim for payment of damages caused by the test and brought to him by a third party (or the client). In the event of third-party claims, the client assumes them, leaving the pentester out of harm's way.

If a contracting party limits or excludes its own liability, this is legally called exoneration. The use of an indemnification and exoneration clause in general terms and conditions is subject to the frameworks of the Civil Code.

This does not alter the fact that any (offensive) digital security test commissioned must always be carried out with care. 'The contractor will have to exercise the care of a good contractor in carrying out his work,' according to Article 401 of the Civil Code.

This involves acting in accordance with objective quality requirements that may be imposed on a reasonably competent and reasonably acting pentester in the concrete case. This is an open minimum standard. It is tested against the level of an average professional, unless otherwise indicated.

It requires, for example, that the pen tester not unnecessarily expose his client to foreseeable and avoidable risks. Moreover, there is the possibility that a pen tester may indemnify his client against third-party claims if, for example, he acted outside the agreed scope or is otherwise grossly at fault in an incident. In that case, the pen tester handles the third-party claims.

Both the element of explicit consent and indemnification may depend in part on the technical resources (tooling, such as scanning software) used in conducting a pen test. Theory and practice show that the scope of a digital security investigation is often not discovered or determined until scans are performed.

This then means that consenting and indemnifying execution is sometimes an iterative process rather than a one-time, prior action based on established data. It is then a process of repeated decisions that requires continuous attention from a decision-maker or manager of the organization being tested (client); someone who has this responsibility formally and is authorized to give permission to scan an object at some level.

Processor Agreement

When outsourcing a digital security test, it is often inevitable to conclude a processor agreement in the sense of the GDPR with the external pen tester in addition to the assignment agreement. This has to do with the possibility that the researcher may unexpectedly gain access to personal data processed by the client while conducting the test.

The law requires that if a controller (client) engages a processor (external pentester) to process data on their behalf, there must be a written agreement that sets out the responsibilities and obligations of both parties (Art. 28 GDPR). The agreement must contain specific provisions on, among other things, the nature and purpose of the processing, the duration of the processing and the types of personal data being processed.

In addition, also in this context, it is important to realize that the law defines data processing broadly, meaning that almost any action involving personal data falls under the term "processing”.

> *"any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data" (Article 4(2) of the GDPR).*

This includes, for example, reading, copying, or analyzing data during a penetration test. In the case of outsourcing, the client (for example, of a penetration test) remains at all times responsible for the personal data they process.

The GDPR requires the conclusion of a processor agreement when outsourcing the processing of personal data. In this context, the client is considered the data controller and the researcher the processor (Article 28 of the GDPRAVG); a view confirmed by a privacy regulator in an EU member state.

Without a processor agreement, the pentester lacks a processing basis and may violate the law when appropriate.

Under the processing agreement, the pentester obtains prior consent to download any personal data, supplemented by the obligation to then irreversibly destroy or return the data at the client's option.

Copyright aspects

Digital technology, such as computer programs, are generally subject to intellectual property rights. In this regard, computer programs in various forms and the copyright applicable to them play a predominant role for both suppliers and user organizations. Most software used by an organization is licensed by the copyright owner and/or authorized supplier.

The legal relationship between parties is governed by statutory copyright (Articles 45h-45n of the Copyright Act), the user agreement and other arrangements such as those laid down in a maintenance agreement.

Conducting a penetration test on software (computer code) to which someone else owns the property rights raises the question of whether this requires permission from the copyright holder. These intellectual property laws grant strong protection rights to the creator. The rights holder can have exclusive possession of his own work.

Copyright is the exclusive right of the creator or his assignees to disclose and reproduce computer code, subject to the restrictions imposed by law (Article 1 of the Copyright Act). This also applies to software: operating systems, application software and interfaces, such as user interfaces (UI) and application programming interfaces (API).

The law names and regulates the testing of a computer program. The lawful user (licensee) may test the producer's software, but these actions must be limited to finding out the ideas and principles underlying the software (Article 45l of the Copyright Act). An investigation of security flaws is in principle not covered by this.

Dutch law has no explicit exception for security research, but performing a penetration test without making copies or distributing the software under investigation falls in principle within the framework of the Copyright Act. This is because no exclusive rights of the copyright holder are infringed in this way.

However, it is important that technical protection measures, such as Digital Rights Management (DRM), should not be circumvented, as this violates copyright protection and is considered an impermissible act under the Copyright Act.

According to the Copyright Act (Article 45j(1) of the Copyright Act), the person who is authorized to use a computer program (licensee) may, "without the permission of the copyright holder, perform all acts necessary for the use of the computer program in accordance with its intended purpose, including the correction of errors.

In principle, this implies that certain forms of testing, such as identifying security flaws, can fall under necessary use and thus do not require separate permission from the copyright holder. In case the performance of a penetration test does qualify as reproduction, especially if temporary copies of the software are

made. In that case, prior permission from the copyright holder of the computer code is legally necessary.

Right to error correction by licensees

Security research can lead to the identification of vulnerabilities, which findings then call for action to improve the security of digital technology and processes, including by fixing flaws in software. Under contract law, the software producer is in principle obliged to remedy defects in a computer program if the computer code does not comply with the defined specifications, which includes security defects. This obligation is based on legal provisions such as the conformity requirement, the rules around defects and the principles of reasonableness and fairness.

However, through the terms of use (license agreement) and general terms and conditions, software manufacturers try to dilute their obligation. This is done, for example, by including clauses stating that the computer program provided is not error-free and cannot operate without interruption.

Also, sometimes a computer program is provided 'as is' ('as is'), without any warranties or guarantees, express or implied, as to the quality, functionality or suitability of the product. In addition, the following clause is common: "The manufacturer shall not be liable for any damages resulting from the use of the software, including but not limited to interruptions or errors in the software.” However, the enforceability of such clauses can

vary. In some cases, such as consumer contracts or gross negligence, such clauses may be limited or invalidated.

Be that as it may, the 2018 Coordinated Vulnerability Disclosure Guideline of the Netherlands assumes a 60-day deadline for the producer to fix the vulnerability.

> *“A CVD policy attempts to strike a balance between the importance of disclosing vulnerabilities as quickly as possible so that measures can be taken, and the interest of developers and vendors in having sufficient time to fix the vulnerability. The NCSC uses a standard period of 60 days between notification and public disclosure for this process. However, there may be circumstances that result in a decision to extend or shorten this period.”*

Individual software users and user organizations also have rights that cannot be waived by contract. In the context of improving information security aspects of software, the usually underexposed European right to error recovery by the licensee has been mentioned.

Every legitimate user possesses, among other things, the inalienable, legally enshrined right to reproduce a computer program in the context of loading, imaging or correcting errors (Article 45j of the Copyrights Act). This right is essential for ensuring the functionality and security of software. A caveat is appropriate here. Licensees usually do not have the source

code of the computer program, unless it is open-source software or if arrangements have been made for a source code repository (software escrow).

Without the software in source code language, error correction (such as bug fixing) becomes very difficult. Those who nevertheless want to have the source code must decompile the machine language (object code, which consists of zeros and ones). This converts the computer-readable form into a human-readable and modifiable form. This process is called reverse engineering.

This act is permitted by law for a lawful user (licensee) only for the creation of interoperable software (Article 45m of the Copyright Act). In other words, the legal right to decompile the object code does not apply for testing purposes or fixing a security bug, unless explicitly granted in the license agreement.

Recently, however, the European courts have taken a different view of this prohibition, specifically with respect to the repair of security flaws. This is an important ruling partly in light of penetration testing. The software under investigation can be modified in response to findings to fix security and functional problems.

Any licensee of a computer program also has the right under the law, according to the European court, to decompile the object code in order to correct errors which affect its operation, including when the correction consists of deactivating a function which interferes with the proper functioning of the application of which the program is a part.

The only limitation the courts place on this rule is that the licensee may perform such de-compilation only to the extent necessary for such improvement and, where appropriate, subject to the terms and conditions established by agreement with the copyright owner of such program.

Automated work (criminal law)

Under certain circumstances, conducting a pen test or other offensive security research, both with and without authorization may enter the realm of criminal law. In particular, this involves the criminalization of acts under the heading of computer crime. Computer crimes often involve the component "automated work". The legal development of the definition of an automated work under Art. 80sexies of the Criminal Code is as follows:

> *“Automated work means a device intended to store and process data by electronic means.”*

March 1, 1993, Computer Crime Act.

> *“Automated work means a device intended to store, process and transmit data by electronic means.”*

Sept. 1, 2006, Computer Crime Act II

> *“Automated work means a device or group of interconnected or related devices, one or more of which automatically process computer data on the basis of a program'.”*

March 1, 2019, Computer Crime Act III

To this the "network" element has been added compared to the previous 2006 version, but the basic premise that it is physical equipment remains unchanged.

Important in this context is the Supreme Court's ruling of March 19, 2024 (GP website), in which the highest court, following the Court of Appeal of The Hague, expressly separated the website from the physical equipment necessary for a website to function.

The Supreme Court states that a website actually consists of a compilation of data, has no physical form and therefore lacks the character of a device. Among other things, the view has implications for the offense of computer hacking (art. 138ab of the Criminal Code), of which an "automated work" (or part thereof) is expressly a part.

> *“He who intentionally and unlawfully intrudes into an automated work or part thereof shall be punished with imprisonment of not more than two years or a fine of the fourth category as guilty of computer hacking. Intrusion shall be*

deemed to have occurred in any case if access to the work is gained:

a. by breaching a security,

b. by technical intervention,

c. using false signals or a false key, or

d. by assuming a false capacity.”

According to legislative history, "computerized work" should be understood to include only physical devices, whereas the offence of computer hacking is always about protecting a (secure) device and not the data even processed in it.

According to the Court of Appeal of The Hague (after referring to case law of the Supreme Court): “It can be deduced from the above that an automated work always includes a (part of a) physical device. So, a computer, server, router, ereader, chip or whatever, but in any case, so-called hardware. In all cases it does not include software, such as computer programs, or websites relevant to the present case (...)”.

In the words of the Dutch Supreme Court: “Since a website actually consists only of a combination of data, does not have a physical form and therefore lacks the character of a device, there is sufficient reason on the basis of the foregoing not to regard a website as an automated work.” An acquittal followed in this case.

The ruling implies that Web sites must be designed differently to qualify for criminal protection. This can be achieved, for example, through the integration of automated components, such as the addition of servers and routers specific to and supporting the website. In addition, the architecture can be modified by creating a dependency on physical devices for data processing. Furthermore, functionality can be added that intentionally uses automated systems, such as real-time data analysis and automatic updates.

Unauthorized access

An offensive security test conducted without the consent of the organization that is the subject of investigation may result in a digital intrusion (hack) or attempted intrusion committed by the pen tester. The first question that arises concerns the legality of possessing technical devices (tools) that can be used to gain unauthorized access to secure networks and information systems.

The Dutch Penal Code makes punishable the manufacture, sale, acquisition, import, distribution or otherwise making available or having at one's disposal a 'technical tool that is primarily suited or designed to commit computer hacking' (Art. 139d para. 2 {Penal Code). A tool used by the pentester in his investigation may in principle fall under such a 'technical aid,' but two criteria must be met. The tool must:

- "primarily" made or designed for hacking: and

- made, owned and more, with the intent to hack.

The criteria generally allow both the organization that conducts penetration testing internally and a professional service provider that tests on commission sufficient leeway to lawfully deploy tools, such as scanning software, in offensive security testing, provided the testing is done with explicit consent and without unlawful intent. As mentioned above, the Supreme Court now does not consider (certain) websites to be an "automated work" in the context of criminal law. This means that, in principle, scanning a website without the consent of the organization under investigation also cannot be legally classified as (an attempted) computer breach. However, this may be different when hacking a computer, server, router, e-reader, chip or other equipment, as well as, for example, a website such as Outlook Web Access (OWA). The Rotterdam court considers OWA to be more than just a website/user interface and states that several technical components are needed to use the web version of Outlook, such as network equipment, an operating system, the application layer and the database servers.

In addition, it is important to emphasize that the Supreme Court ruling does not necessarily mean that all forms of unauthorized scanning or other interactions with Web sites are legally permissible under criminal, privacy, copyright or contract law. For example, unauthorized scanning of a website may result in unlawful processing of personal data or copyright infringement of software.

For completeness, since the entry into force of the Computer Crime Act III on March 1, 2019, the police have the power to surreptitiously penetrate a suspect's automated work (Article 126nba Dutch Code of Criminal Procedure), such as a laptop or smartphone. Again, this legal hacking power is an offensive tool, which is also subject to strict conditions and may only be used in case of suspicion of a serious crime.

Coordinated Vulnerability Disclosure

An ethical hacker who researches vulnerabilities in third-party ICT systems without explicit permission and unlawful intent may be in legal trouble. From a public interest perspective, this situation calls for the protection of individuals acting in good faith. This is why some countries have established policies or regulations for reporting digital security problems discovered in this way. In the Netherlands, the guideline Coordinated Vulnerability Disclosure (2018) of the Dutch National Cyber Security Center (NCSC) is in place.

According to the Public Prosecutor's Office (OM), it is important for hackers to be able to continue to find and report vulnerabilities so that ICT systems can be made more secure. Therefore, the OM encourages organizations to adopt policies on reporting vulnerabilities in their ICT systems.

Note that such a CVD scheme binds both the organizations and the reporter. Investigators are advised by the OM to keep track of their steps in a log file to demonstrate compliance.

This policy attempts to strike a balance between the importance of disclosing vulnerabilities quickly so that appropriate action can be taken, and the interest of developers and vendors in having sufficient time to fix the vulnerability.

The Netherlands has a dual policy. Anyone who finds a technical vulnerability in a central government system can report it to the NCSC. If it concerns a vulnerability in digital technology of another organization, the discoverer should first approach the owner of the system or the product supplier. Only if this organization does not respond, or does not respond adequately, can the discoverer report the vulnerability to the NCSC, which then acts as an intermediary and reports the vulnerability to the organization in question. In this regard, caveats are appropriate. The CVD policy of OM and NCSC stands or falls with an applicable CVD regulation per organization. For central government organizations, these regulations are uniformly available. This probably does not apply to every healthcare institution, for example.

Organizations that have not yet created and published a CVD policy would do well to include it as part of their information security policy. In the absence of such a regulation, those involved (pen tester, organization under investigation and OM) fall back on the general policy and legal rules because the requirements of ethical hacking have not been met.

Another note concerns a related confidentiality issue, namely an obligation often included in employment contracts. If employees examine their own organization at management's request and the findings that require action do not lead to

information security improvements, an employee may end up being considered a whistleblower due to disclosure of the test results. Dutch law has had the Whistleblower Act since July 1, 2016, which regulation is currently being revised under European law.

It is also important to note that while an organization's CVD policy in principle exempts an ethical hacker from criminal liability, it does not exempt him from civil or administrative liability. Examples of civil liability include claims for damages from the hacked organization, while administrative liability may include a fine from a regulator for a breach of privacy or AI law.

To date, CVD policy in the Netherlands is a form of self-regulation, as legislation does not require it. That said, the BIO does mandate having a Coordinated Vulnerability Disclosure procedure for every government agency (Article 16.1.3.1 of the BIO).

This situation is changed by the NIS2 Directive. According to the directive, coordinated vulnerability disclosure designates "a structured process by which vulnerabilities are reported to the manufacturer or provider of the potentially vulnerable ICT products or ICT services in a manner that enables it to diagnose and remediate the vulnerability before disclosing detailed information about the vulnerability to third parties or to the public" (Recital 58 of the NIS2).

First, by Oct. 18, 2024, member states must formulate, adopt and implement vulnerability management policies as part of their national cybersecurity strategy, which includes the

promotion and facilitation of coordinated vulnerability reporting under Article 12(1) of the NIS2).

An important element of this policy is the role assigned at the national level to at least one Computer Security Incident Response Team (CSIRT) to act as coordinator for the purposes of CVD and receiving reports of vulnerabilities (Article 12(1) and 11(3)(g) of the NIS2).

In addition to the new legal obligations at the country level, essential and important entities, including central government organizations, must implement technical, operational and organizational cybersecurity risk management measures (Article 21 of the NIS2). This legal duty of care explicitly includes vulnerability management ("vulnerability handling") and incident reporting procedures ("incident reporting").

Forensic evidence

Forensic research helps identify perpetrators or the causes of (possible) crimes or offenses based on scientific evidence, usually with the help of technology. This type of truth-finding research can be carried out by the police and special government research institutes, such as the Netherlands Forensic Institute (NFI), as well as private investigators. The results of the investigation can serve as evidence in criminal proceedings.

One of the many areas within forensic science involves digital trace evidence, that is, investigation of digital traces and data that are in principle impossible or difficult to retrieve by other means. Digital evidence also aims to provide certainty about alleged facts. Researchers secure and analyze the traces. This field, also called computer forensics ("digital forensics"), has been increasing in scope and importance for years.

Although forensic or judicial investigation is typically primarily associated with criminal justice, forensic computing can be applied more broadly, specifically for finding legal evidence in and from computers, software, networks, websites, and, for example, storage media, serving the entire legal and policy spectrum.

This includes private, administrative or public law issues in addition to criminal law. In other words, forensic informatics today no longer focuses exclusively on digital evidence for the purpose of investigating crimes and prosecuting suspects.

The underlying rationale is important. After all, unlocking, securing and analyzing digital traces for scientific evidence can relate to almost anything. This can range from establishing violations of intellectual property rights to breach of contract by an opposing party, or verifying security measures, including digital ones. This applies in any legal relationship: between citizens and businesses, between citizens and businesses, and between government organizations.

During a penetration test, digital technology and/or processes are examined for vulnerabilities through offensive scanning. The findings essentially consist of electronic data and can be used as digital traces in a forensic investigation.

On the one hand, it concerns the production of digital evidence: the way in which evidence is created, collected and how the strength of that evidence is established. On the other hand, evidence must be secured: the assurance that the evidence produced can actually be used as such, for example in legal proceedings.

Depending in part on the tools used, methodologies followed, standardized reporting and their review by an IT auditor, the findings of a penetration test can lead to conclusive, recognized scientific evidence.

Legal Developments

Practice shows that one vulnerability is not the same as another. Among other things, a distinction is made between common and critical variants, related to the potential impact and severity of the vulnerability. In addition, vulnerabilities are classified as "known" and "zero-day" vulnerabilities.

A zero-day vulnerability is generally described as a security flaw unknown to the software or hardware developers at the time it is discovered or exploited. Because the vulnerability is unknown to the responsible parties, they have not had time ("zero time") to develop a patch or fix, which explains the name.

One note here is that vulnerabilities are usually associated with the confidentiality of data processing, while information security also relates to the core concepts of availability and integrity.

Many standards organizations link a vulnerability to the circumstance that it can be exploited. In other words, if a weakness or flaw cannot be attacked (for example, with specially written computer code or an "exploit") or otherwise exploited, it is apparently not considered a vulnerability.

However, it is important to recognize that not all vulnerabilities require direct exploitation by an attacker to pose a threat. Autonomous system failures, software bugs and operational risks (the result of both intentional acts and omissions) can be just as damaging and should therefore be taken seriously in the context of information security, as should intentionally acts by malicious actors.

The US federal organizations NIST (in SP 800-30) and the European agency ENISA take a broader definition of a vulnerability and consider a vulnerability to be a technical weakness that in practice can lead to a security problem, whether accidental or through intentional misuse. This approach deserves support, as any kind of flaw with a digital security risk in principle requires action, regardless of intent. Meanwhile, the European legislator is also on this line. As mentioned, the NIS2 defines "vulnerability" as follows:

> *" a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber*
>
> *threat " (Article 6(15) of the NIS2).*

A "cyber threat" should then be taken to mean the Cybersecurity Act (CSA):

> *" Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons " (Art. 2(8) of the CSA).*

Both are broad definitions. Further important is the EU Cybersecurity Resilience Act (CRA). This regulation deals with security measures for a "*product with digital elements*," that is, "*any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately*" (Article 3(1) of the CRA).

Products with digital elements must be designed, developed and produced according to security requirements so that they ensure an appropriate level of information security based on the risks and must be delivered without known vulnerabilities that can be exploited. In doing so, extensive testing is unavoidable. The design distinguishes into three product categories with digital elements, related to the critical status of the application: ordinary, critical and high-critical.

It is noteworthy that the Dutch Guideline Coordinated Vulnerability Disclosure (CVD) does not use a definition of a vulnerability and does not refer to the European law definition.

The NCSC uses a standard 60-day period between the CVD notification and the public disclosure for fixing the vulnerability.

Another legal development comes from consumer law. To ensure proper and safe use, providers of a digital product or service are obliged under the Digital Content Delivery Directive (Article 7:50a to 7:50f of the Civil Code) and the Sale of Goods Directive (Article 7:18 to 7:23 of the Civil Code) to provide software updates, expressly including security updates.

In 2017, the Dutch Minister of Justice and Security wanted to take action against digitally insecure companies that failed to promptly install a 'security patch,' but this plan did not lead to new regulation. In 2019, this minister was again considering intervening in the market, this time because vital providers were apparently not sufficiently following security recommendations:

> *“Where necessary, use will be made of the intervention options under the Wbni when necessary, in the context of national security. For example, the NCSC will more often inform regulators of situations in which a vital provider does not adequately follow security advice, leaving risks to national security. The VPN-Pulse vulnerability shows that warnings and advice from the NCSC are not always followed immediately.”*

The issue of liability in relation to a vulnerability begins with the question of who is responsible for what. There is agreement on

this to the extent that, according to the Minister of Justice and Security, organizations are primarily responsible for their own cybersecurity, while software manufacturers are primarily responsible for the digital security of the products and services they offer. This is in line with views of others, such as the Dutch Safety Board (OVV) to which the Parliamentary questions relate.

Flaws in software, including security flaws, can lead to liability for damages arising from them, under both the doctrine of tort and culpable failure (breach of contract) in the performance of a contract. In both cases, the vulnerability must be imputed to someone. Case law on digital vulnerabilities under Dutch law is virtually non-existent.

To encourage software producers to do more about information security, the Rutte III administration wanted to introduce special legal liability for insecure software into Dutch law. This policy intention, set out in the coalition agreement of Oct. 10, 2017, was not implemented.

Instead, the minister stressed the importance of making quality and liability agreements at the international and European level on digital security, due to the cross-border nature of the market for ICT products and services. This is in line with the recommendations of the Dutch Safety Board (OVV).

Already mentioned is the Cyber Resilience Act (CRA), the regulation aimed at establishing common information security standards for products with digital elements (product safety). Furthermore, the EU is working on the revision of the Product Liability Directive, which aims to adapt the rules on this to the digital and circular economy, as well as modern technological developments such as artificial intelligence (AI).

Last but not least, the Common Vulnerabilities and Exposures (CVE) list has been used worldwide since 1999. This list, created by the MITRE Corp. in cooperation with the international information security community, assigns vulnerabilities a unique identification number. This number makes it easier to track vulnerabilities, exchange information and assess computer code. Recognized by security experts, governments and companies worldwide, the CVE system promotes international cooperation and standardization in information security.

In addition, the CVE system contributes to a standardized and structured approach to identifying and managing vulnerabilities, resulting in improved information security. The CVE list enables software producers to continuously identify and fix known vulnerabilities. The CVE list is often used in conjunction with other security databases, such as the National Vulnerability Database (NVD), which provides additional details and context about vulnerabilities.

Conclusions

Digital quality deficiencies, such as vulnerabilities (legally defined as "w weakness, susceptibility or flaw of an asset, system, process or control that can be exploited "), make individual users, organizations and society vulnerable. On the one hand, a shortcoming in relation to ICT facilitates the

execution of cybercrimes; on the other hand, vulnerabilities autonomously and unintentionally increase the risk of disruption and failure of business processes.

Every organization, regardless of sector and size, because of the social importance of digital resilience, has a legal duty of care for information security. This focuses on taking organizational, technical and operational risk management measures to ensure the confidentiality, continuity and availability of the data processing for which the organization is responsible.

Central government organizations are also subject to the obligation to implement policy rules, as set forth in, among other things, the Central Government Information Security Regulations Decree 2007 (VIR 2007), the Central Government Information Security Regulations Decree - Special Information (VIR-BI 2013) and the Government Information Security Baseline (BIO).

This legal duty of care includes monitoring and accountability for the implementation, compliance and ongoing adequacy of the risk management measures in place. The NIS2 Directive explicitly states this.

Organizations under its scope and that of the upcoming Dutch Cyber Security Act (Cbw) must have policies and procedures "*to assess the effectiveness of cyber security risk management measures*" (Article 21(2)(f) of the NIS2). In addition, security incidents must be monitored and addressed (Article 21(2)(b) of the NIS2). The same applies under privacy laws, among other things.

Digital security investigations, such as penetration testing, are crucial to a proactive approach to information security. This type of testing helps organizations identify and address vulnerabilities in their systems before malicious actors can exploit them or before the wakes otherwise lead to problems.

Reactive penetration testing should then occur after an incident to identify the cause, assess the extent of the damage and implement appropriate measures to prevent recurrence. Law plays an important role in each case.

Performing penetration tests with legal care facilitates both compliance with duties of care and other legal, policy and contractual requirements (legal compliance) and effective execution within legal frameworks (value creation). Both aspects contribute to strengthening digital resilience and reducing the risk of legal and political liability.

Sample questions for clients

General requirements

- Can you confirm that the report will be provided in digital form?
- Will the name of the rapporteur, certifications (e.g., OSCP, OSCE) and contact information be included in the report?
- How do you ensure that the report is accurate and truthful?
- What version control system or method is used to track changes to the report during preparation?
- Is the digital signature of the rapporteur provided with the report?

Pentest Execution Standard (PTES).

- Can you confirm that your research was conducted according to the seven phases of PTES: Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation and Reporting?
- Will the report detail this format for each phase?
- How do you ensure that all necessary information is collected during each phase to support findings and recommendations?

- Can you confirm that your research was conducted according to industry best practices (e.g. NIST Cybersecurity Framework)?

- Are there specific PTES phases or activities where additional guidance or resources have been sought from outside experts?

Confidentiality

- How do you ensure that confidentiality agreements made prior to the investigation are properly documented in the report?
- Will all affected parties (e.g., clients, stakeholders) be informed of their obligations under these agreements?
- Are there specific procedures for handling confidential information or sensitive data collected during your research?
- Can you confirm that a clear and concise summary of the confidentiality agreement will be included in the management summary of the report?
- How do you ensure compliance with relevant laws, regulations and industry standards (e.g., GDPR) when collecting and storing personal data?

Intake interview and Action Plan

- Will the offer include a record of the intake discussion, including names, date, participants and key points or action items agreed upon during the discussion?

- Will the report include a record of the intake discussion, including names, date, participants and key points or action items agreed upon during the discussion?
- Can you confirm that any changes in scope or requirements made after the original intake interview were properly documented in writing (e.g., via email or formal memo)?
- Will a clear and concise summary of expectations, needs and priorities be included in the management summary of the report?

Scoped definition and research methodology

- Can you confirm that the scope of the study was clearly defined in writing before you began your research?
- If infra/web application: How do you ensure that all objects identified within the scope are tested with a combination of manual testing (e.g. OWASP Web Application Security Testing Guide, WSTG) and automated tools (e.g. Nessus)?
- If mobile: Will the report include a description of how mobile application testing was performed for each scope object?
- How do you ensure compliance with relevant standards (e.g., PTES, NIST Cybersecurity Framework) when performing the pen test?

Standard: OWASP Firmware Security Test

- Will the report include a description of how OWASP Firmware Security Testing was performed for each scope object?

- Can you confirm that any firmware security tests conducted during your investigation met relevant standards (e.g., PTES, NIST Cybersecurity Framework)?
- How do you ensure compliance with industry best practices when conducting firmware security reviews?
- Will the report include a summary of findings related to firmware security vulnerabilities or weaknesses identified during your investigation?
- Can you confirm that any recommendations regarding firmware security testing are properly documented and prioritized based on risk?

Standard: OWASP Web Application Security Testing Guide (WSTG)

- How do you ensure compliance with WSTG guidelines when performing Web application penetration testing for each scope object?
- Will the report include a description of how manual tests were performed using WSTG techniques for each scope object?
- Can you confirm that any automated tools used during your research (e.g., Nessus) were correctly configured to follow WSTG best practices?
- How do you ensure compliance with industry standards when performing Web application security assessments for each scope object?
- Does the report include a summary of findings related to Web application vulnerabilities or weaknesses identified during your investigation?

Standard: OWASP Mobile Application Security Testing Guide (MASTG)

- Can you confirm that any mobile application tests conducted during your study complied with relevant MASTG guidelines and best practices?
- How do you ensure compliance with industry standards when performing mobile application security assessments for each scope object?
- Will the report include a description of how manual tests were performed using MASTG techniques for each scope object?
- Can you confirm that any automated tools used during your research (e.g., MobSF) were correctly configured to follow MASTG best practices?
- How do you ensure compliance with relevant standards when conducting mobile application security assessments?

Standard: Common Vulnerability Scoring System (CVSS).

- Will the report include a description of how CVSS scores and vector strings are calculated for each recorded finding?
- Can you confirm that any CVSS calculations performed during your study complied with relevant industry guidelines or best practices?
- How do you ensure compliance with CVSS standards when documenting findings related to security vulnerabilities or weaknesses identified during your investigation?

- Will the report include a summary of findings related to security vulnerabilities or weaknesses identified during your investigation, including their associated CVSS scores and vector strings?
- Can you confirm that any recommendations related to mitigating or fixing security vulnerabilities are properly documented and prioritized based on risk?

Standard: Common Weakness Enumeration (CWE).

- Will the report include a description of how CWE items are used for each recorded finding related to identified security weaknesses during your investigation?
- Can you confirm that any CWE items used during your study complied with relevant industry guidelines or best practices?
- How do you ensure compliance with CWE standards when documenting findings related to security vulnerabilities or weaknesses identified during your investigation?
- Will the report include a summary of findings related to security vulnerabilities or weaknesses identified during your investigation, including their corresponding CVSS scores and vector strings?
- Can you confirm that any recommendations related to mitigating or fixing security vulnerabilities are properly documented and prioritized based on risk?

Tools used during the study

- Will the report include a description of all tools used during your investigation (e.g., Nessus, nmap)?

- How do you ensure compliance with industry standards when using automated tools to perform vulnerability assessments for each scope object?
- Can you confirm that any findings regarding security vulnerabilities or weaknesses identified during your investigation were properly documented and prioritized based on risk?
- Will the report include a summary of findings related to security vulnerabilities or weaknesses identified during your investigation, including their corresponding CVSS scores and vector strings?
- How do you ensure compliance with industry standards when documenting findings related to security vulnerabilities or weaknesses identified during your investigation?

Appendices and glossary

- Does the report include all attachments (e.g., screenshots) generated during your research?
- Can you confirm that any SHA-1 hashes included in the report were calculated correctly for each attachment?
- How do you ensure compliance with industry standards when documenting findings related to security vulnerabilities or weaknesses identified during your investigation?
- Will the report include a glossary of terms used throughout the document (e.g., technical terms)?

- Can you confirm that any recommendations related to mitigating or fixing security vulnerabilities are properly documented and prioritized based on risk?

Scan results, evidence and checklists

- Will the report include scan results from scans performed during your research?
- How do you ensure compliance with industry standards when documenting findings related to security vulnerabilities or weaknesses identified during your investigation?
- Can you confirm that any evidence generated or created by your team is properly documented (e.g. SHA-1 hashes)?
- Will the report include a summary of findings related to security vulnerabilities or weaknesses identified during your investigation, including their corresponding CVSS scores and vector strings?
- How do you ensure compliance with industry standards when documenting findings related to security vulnerabilities or weaknesses identified during your investigation?

Technical inaccessibility

- Can you confirm that any scope objects found to be technically inaccessible were correctly documented in writing at the time of investigation?
- Will the report include a description of how technical inaccessibility was determined for each affected scope object?
- How do you ensure compliance with industry standards when documenting findings related to security vulnerabilities or weaknesses identified during your investigation?
- Can you confirm that any recommendations related to mitigating or fixing security vulnerabilities are properly documented and prioritized based on risk?
- Will the report include a summary of findings related to security vulnerabilities or weaknesses identified during your investigation, including their corresponding CVSS scores and vector strings?