Policy / Instruction

Costumer Policy for Security Assessments and Penetration Testing

Document Nr.
18 External

Document Name
Costumer Policy for Security

Version/Date
Version 3.0, 23.10.2024

Classification
Public

Release Date
[30.10.2024]

Area of Application
External Entities

Green Datacenter AG • Industriestrasse 33 • 5242 Lupfig • Switzerland
+41 56 460 23 80 • business@green.ch • www.green.ch

Table of Contents

1 Introduction

In today's digital age, most technical devices are able to be constantly connected and accessible. This increases the complexity of managing them and at the same time increases the potential attack surface for a company. For this reason, it is important to regularly check a company's infrastructure for technical deficiencies. This process should be accomplished with penetration tests.

1.1 Purpose

As a provider of critical infrastructure, we welcome our customers to conduct security tests on parts of Green's infrastructure and services.
It is to be stated, that not all types of testing are allowed to be conducted and some parts of the Green's infrastructure and services are off-limit. This policy shall provide an overview of what is allowed and else strictly prohibited.

Please ensure that any activities are aligned with the policy set out in the following chapters. Should your testing activities result in any disruption of service, we reserve the right to take measures to protect the service, which may include shutting down or blocking your tenant and/or the source of the intrusion traffic.

1.2 Applicability

This policy applies to all external entities conducting penetration tests or operations alike on Green's infrastructure and/or services.
It is applicable to all of the assets of Green, with the exception of the OT-environment, which should be considered off-limit if not else defined in conversation with Green.
The asset inventory includes (among other) non-connected and connected devices and cloud-based appli-cations.
All penetration tests performed on devices owned and controlled by Green must comply with all national and regional laws governing the physical location of the device and the nature of the data, as well as any restrictions on acceptable use imposed by contracts and agreements between Green and third-party pro-viders of infrastructure services and application licenses.
It should also be noted that this policy does not contain a comprehensive definition of all scenarios and activities that may occur during penetration testing. Therefore, all parties involved should use their best judgment when conducting penetration tests and use the defined communication channels to clarify potentially conflicting situations.

1.3 Goals

The main goal of this policy is to determine vulnerabilities in company systems, which may endanger the confidentiality, integrity or availability of said systems.
Ultimately, the identification of weaknesses should facilitate the elimination of risks in line with the company's internal management objectives.

1.4 Reference

CIS Control 18.2	Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be white-box or black-box.	IG1 IG2 IG3

2 Scopes of Penetration Test

Penetration tests can be have different scopes and take place in different locations. The following text shall provide a list of the types of penetration tests.

2.1 Network

Network penetration tests are done to locate vulnerabilities and security flaws in the network infrastructure of Green. Being part of said network infrastructure are (amond others) servers, firewalls, routers, switches, printers, peripherals and any network applications and -API.
Network penetration tests may occur with or without access to any credentials provided by Green.

2.2 Web Applications

Penetration tests of web-applications are used as a way to locate exposed vulnerabilities and security flaws in the web-applications run under Green's infrastructure.
Such tests are mostly conducted with the usage of already known and malicious attack methods during manual and also automatic testing.

Guidelines such as framework like from OWASP «OWASP Top Ten web-application vulnerabilities», the list «CWE Top 25 Most Dangerous Software Weaknesses» compiled by MITRE and the MITRE ATT&CK framework shall serve as a foundation for the web-application penetration tests.

- OWASP Top Ten web-application vulnerabilities - https://owasp.org/www-project-top-ten/
- MITRE CWE Top 25 Most Dangerous Software Weaknesses - https://cwe.mitre.org/top25/
- MITRE ATT&CK Framework - https://attack.mitre.org

2.3 Social Engineering

Conducting a social engineering campaign on Green's employees is strictly prohibited. It is however desirable, that the pentester discusses possible ideas and gives feedback to the internal employe(s) responsible for the company's social engineering campaigns.

3 Policy

3.1 Scope and Limitations

In advance of any penetration test, the scope and limitations under which the attacker shall operate are to be defined. Each contract may also include specific requirements and contractual obligations, such as service level agreements (SLAs) with Green's customers and users and compliance with formal IT security standards. The scope of each assignment must also not exceed the limits of the applicable national or regional regulations or Green's contractual obligations.
The CSCC team leader shall keep a record of the aforementioned limitations in a separate document. Said document shall then be reviewed and signed by the CIO.
The inventory list is to be handed over to the pentester enough in advance of the time the audit is taking place.

3.1.1 Regulations and Rules of Conduct

The penetration tester acts as a simulated attacker and is responsible for the practical execution of the penetration test. He is obliged to operate only within the national and regional legal area permitted by the company.
Possibly found security vulnerabilities are to be reported to Green and are not to be shared under any circumstances with third parties.

3.1.2 Penetration Testing Request

Green customers are welcome to carry out security assessments or penetration tests against their own infrastructure without a prior written approval by Green and/or Green Datacenter.

To conduct a security assessment or penetration test against Green or GDC infrastructure and services, we require at least 10 working days' notice prior the start of the test.

Please provide the following information when requesting approval for testing:

- *The specific dates/times of the test in CET time zone*
- *Scope and purpose of the test*
- *All IP address(es) the test data will be coming from*
- *Tools and methods that are planned to be used*
- *Phone number and Email of at least two contacts who will be available during the entire test period in case we need to contact you*

3.1.3 Penetration Testing Time Windows

It is requested that all tests are performed during green office hours in case emergency support is required. Always consult our website for the most current opening hours.

3.1.4 Permitted Services and Infrastructure

To protect our other customers and to not distort your test results we request you to limit your testing in accordance to our externally curated list, containing all services from Green and GDC and its infrastructure allowed to be tested. The named document is to be handed out by Green to the pentester prior to the start of the audit.

3.1.5 Prohibited Activities

Following activities are strictly prohibited and must without any exceptions not be executed neither on costumer's or Green's infrastructure.

- *Denial of Service (DoS)*
- *Distributed Denial of Service (DDoS)*
- *Simulated DoS*
- *Simulated DDoS*
- *Port Flooding (e.g., SYN Flood Attacks)*
- *Protocol Flooding*

- *Request Flooding (e.g., API request flooding)*
- *In general, any automated testing services that generate significant amounts of traffic*

Furthermore, the following activities are prohibited:

- *Gaining access to data that one don't wholly own or are responsible (as data processor) for*
- *Attempt social engineering attacks against Green's employees or contractors*
- *Using Green's services in any way that violate the contract between a person and Green*

3.1.6 Provided Resources

Depending on the necessity and the type of a penetration test, Green can provide the following elements to the penetration tester:

- **Github**
  - Internal Github repository, which contains an assortment of files related to penetration testing in e.g. documentations and scripts.
  - The repository can be accessed via the following link (private, permission must be granted by the respective owner(s)):
    https://github.com/notapentester1/CSCC_pentest
- **Credentials**
  - Access to the Active Directory
  - Depending on the scope and only after consultation, further accesses may be provided.
- **Inventory List**
  - Includes a curated list of all assets of Green, which are allowed to be pentested
  - It includes a diagram of Green's network infrastructure
- **Report Template**

3.2 Reporting

Green requests a written report from the contractional penetration tester at the end of the penetration test. A template for the report will be provided by Green.

The report should contain at least the following information:

- *A list of the found vulnerabilities (including their CVSS score)*
- *Explanation of the difficulties encountered during the "Exploitation" phase (if any)*
- *Analysis and assessment of the vulnerabilities found and their risks*
- *Recommendations on how Green could handle the vulnerabilities found and fix them if necessary*

3.3 Asset Inventory

A comprehensive list of all assets, which are allowed to be tested during an audit, will be provided as a separate document. The inventory is to be maintained and updated regularly by the CorpIT in a separate document.
So sieht eine Standard-Tabelle einfarbig aus:

4 Exceptions to the Policy

Requests for exceptions to this policy must be submitted to the CSCC department. The CSCC then makes a recommendation to the Chief Information Officer (CIO) regarding the requested exceptions. The CIO reviews the recommendations and approves them if necessary.

Such a request should at least contain the following points:

- *Reason for the request*
- *Risks occurring should Green not follow the exception(s)*
- *List of precautions to minimize the risks that have not already been implemented*
- *Technical and other difficulties*

- *Revision date*

5 Appendix A: Terms and Definitions

- *Black-Box Tests* – Refers to the method of testing systems, where tests are developed without knowledge about the inner workings of said systems
- *CIO* – Chief Operational Officer
- *CVE* - Cybersecurity Vulnerabilities in IT systems that are categorized within the CVE program and made publicly available
- *CSCC* – Cybersecurity Competence Center
- *GDC* – Green Datacenter
- *GDPR* - General Data Protection Regulation
- *Grey-Box Tests* – Refers to a combination of the previously defined white and black box tests. The aim is to find defects in applications and/or in infrastructure, which is caused either by production or usage faults.
- *OT (Operational Technology)* – Describes the software and hardware that detects or causes a change through the direct monitoring and/or control of industrial plants, systems, processes and events. They are usually categorized as infrastructure-critical systems.
- *revDSG* - Neues Datenschutzgesetz
- *White-Box Tests* – Refers to the method of testing systems, where tests are developed with knowledge about the inner workings of said systems