PRODUCT PRESENTATION

QGROUP Check4Hack

Are you safe?

- Holistic overview of the status quo of IT security
- Optimal basis for further budget planning and follow-up action
- Detection of unknown potential dangers and intruders
- Support in the implementation of the Basic Data Protection Regulation

The QGroup was founded in 1993 and among other sectors is active in the areas of military IT security and IT high availability. The company is headquartered in Frankfurt am Main and has employees in the USA and Canada. For General Dynamics, QGroup is the Center of Excellence for Pitbull® Trusted Operating Systems and Multilevel Security. Accordingly, QGroup has many years of experience with customers in the military environment as well as in the official and commercial sectors of high security.

QGroup assists companies with consulting, design and implementation of security concepts. In doing so, it supports them with security analysis, penetration tests and social engineering and maintains a 24/7 Security Incident Response Team for its customers. On top, QGroup transfers pragmatic military security strategies to civilian solutions and customers in order to meet modern security and resilience requirements. QGroup always pursues a holistic approach to security.

In our experience, pure prevention is no longer sufficient. Too often, we notice that the attack against which a company wants to protect itself, has already taken place in the past - companies often don‘t even notice significant attacks. For this reason, we have developed a comprehensive security assessment program, the Check4Hack. Various procedures and approaches are used in combination with highly specialized hardware and software as well as expert knowledge.

In contrast to penetration testing, we not only examine a selection of possible attack vectors, but also get a comprehensive picture of the current compromise, the most critical attack vectors and their elimination options.

Attack vector analysis

Together with the customer, we develop an overview of the existing IT infrastructure. Based on our experience in the military IT security area, we identify attack vectors, which we use in the subsequent tests if necessary.

Network forensics

This module detects advanced persistent threats (APTs), complex malware, exploits and remote command & control. By using the high-end Fidelis Scout active attackers can be detected in real time and analyzed forensically. This makes it transparent which data infiltrates a network or which leave it. Attacks from the past can be detected due to the behavior of compromised devices.

Vulnerability analysis

Based on the results of the attack vector analysis, different vulnerability scans are started on the systems to be tested. The final report gives a critical assessment of the vulnerabilities and misconfigurations found. In addition, possibilities for eliminating these vulnerabilities are shown. The focus here is on establishing the relationship between the investigation results and the financial and business risks in both, a pragmatic and analytical manner and in collaboration with our customers. The result is a clear picture of how much an attacker would have to invest to compromise the company‘s information security.

QGROUP GMBH

QGroup GmbH | Berner Straße 119 | 60437 Frankfurt | Germany
Phone: +49 69 90 50 59 0 | +1 217 377 2001 | E-Mail: info.us@qgroup.de
www.qgroup.de

PRODUCT PRESENTATION

QGROUP Check4Hack

Optional Modules

Password audit

Password security is essential. Company passwords are checked using methods such as brute force, dictionary attack, known initial passwords, and combinations of these methods. The resulting findings provide information as to which of the passwords used are easy to break. In this way, measures can be taken to ensure and control the quality of the passwords.

IoT analysis

One of the most common entry points for hackers today are IoT devices such as surveillance cameras, access points, etc. These devices firmware is rarely patched or not patched at all and are currently often not in the security focus. The QGroup supports you in closing this gap.

Penetration testing

The penetration test usually takes place after the introduction of new (sub)systems in order to check them for their vulnerability or after a Check4Hack in order to manually track the found vulnerabilities and generally to investigate how deep one could penetrate the system. It is repeated regularly to ensure system compliance.

Social hack

What used to be true for top companies and public authorities has now become the norm in the entire economy: espionage and targeted, destructive attacks. The attackers go beyond technical measures - social engineering means are increasingly used, i.e. social attacks on people, to improve the chances of a successful attack. Therefore, in many cases an assessment of an organization's technical defensive capabilities is not enough. For this reason, we offer the QGroup Social Hack, a security check that supplements technical attack vectors with the technology of social engineering. After a social hack has been carried out, holistic improvements for the security of the organisation can be derived and appropriate awareness can be created among the employees.

Optional follow-up actions

- Prioritisation of measures
- Determination of protection requirements
- Creating a Security Policy
- 24/7 Incident Response
- ...

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

QGROUP GMBH

QGroup GmbH | Berner Straße 119 | 60437 Frankfurt am Main
Telefon: +49 69 90 50 59 0 | E-Mail: vertrieb@qgroup.de
www.qgroup.de

PRODUCT PRESENTATION

QGROUP Check4Hack

Optional follow-up

Determination of protection requirements (e.g. according to BSI demands)

Basically, it is still common today to define security parameters more or less according to the experience and intuition of IT departments. A qualified determination of the need for protection, i.e. the objective determination of the level of protection required by an organization's IT, has often not yet taken place, since such a determination must, of course, be implemented within the entire organization on an interdisciplinary basis and can seldom be carried out by IT department personnel alone. We have developed a simple method based on questionnaires to create a so-called protection requirements matrix, which is easily verifiable and later serves as a basis for the creation of a universal security policy. In many projects, the experience of customers and the QGroup has been incorporated in order to reduce the hurdle for determining the need for protection to a minimum.

Prioritization of measures and holistic consulting

In our experience, it is not easy for organizations to deduce the right conclusions and activities from the results of such a comprehensive security assessment as a Check4Hack. Neither can the organization address all the vulnerabilities found at once, nor are budgets planned for them. For this reason, we help our customers with the next steps following Check-4Hack as part of our holistic consulting services. First, a qualified validation of the Check4Hack results is discussed with the customer. Afterwards a prioritization of the possible measures is carried out, as well as a planning for a period of several years. This serves on the one hand to create a solid basis for decision-making, on the other hand to asap eliminate the worst weaknesses with the least possible effort, know-how and experience at very short notice, without overtaxing the organization. Although our customers often have extensive internal security know-how, it is often helpful to plan measures calmly according to the motto: „every small step leads to the goal". This is also shown by the feedback from our customers who have gone through this process.

Creating a security policy

On the basis of the QGroup's determination of protection requirements and best practice approaches, effective protection measures are derived from the military sector and recorded in a security policy that is generally valid for the customer. We often test the security policy on certain systems in order to ensure that it can be implemented in practice. Nevertheless, for commercial reasons, some protection requirements may not immediately be met by appropriate measures. These cases are documented accordingly and transferred to a separate risk list or risk management, for ongoing monitoring and mitigating actions.

24/7 Incident Response

On the basis of the knowledge gained in Check4Hack, the QGroups Incident Response Teams are enabled to immediately initiate the necessary defensive measures to limit the extent of damage in the event of an incident.

The Incident Response Contract includes:

- Access to an Incident Response Team of QGroup, consisting of at least two specialists
- Response times up to 24/7/xh
- One annual Check4Hack (optional quarterly or half-yearly)
- Fixed contingent of man-days
- Reduced daily rate for additional requirements
- No travel costs / accommodation costs

Through the services included in the 24/7 Incident Response, you ensure a constantly increasing IT security in your company.

Trust Seal
www.teletrust.de/itsmig

SecurITy made in Germany

QGROUP GMBH

QGroup GmbH | Berner Straße 119 | 60437 Frankfurt am Main
Telefon: +49 69 90 50 59 0 | E-Mail: vertrieb@qgroup.de
www.qgroup.de