Schedule of Services
Cyber Security Services

TÜV NORD GROUP

Penetration Tests

Contents

1 Introduction

In connection with progressive digitalization and networking, data, systems and business process applications are increasingly exposed across all organizations to the existential threat of cyber-attacks. The continuous maintenance and optimization of the security level envisaged as well as specific compliance requirements demand a sustainable, coordinated and effective combination of organizational and technical security measures.

The Cyber Security Services by TÜV Informationstechnik GmbH (TÜViT) offer a modular range of analytic security services to match your requirements perfectly, so as to objectively assess and increase the security level from simple to complex objects of investigation according to a holistic or focused approach.

Our experts provide professional support for your projects. Established security measures are assessed with regard to their effectiveness and completeness, specific documented risks are highlighted and appropriate action measures proposed for vulnerabilities identified so as to remedy the same. For this purpose, by means of adept penetration tests, attack techniques from the security scene are used that allow an attacker to

- infiltrate the security measures implemented,
- in order to manipulate business processes without authorization,
- to access sensitive data and
- possibly even to endanger human life.

The service portfolio of TÜViT Cyber Security Services can be applied across all sectors and comprises a.o. the following performance characteristics:

- Inspection and consultation services for various objects of analysis
- Penetration tests in connection with APTs and information security revisions (IS-Pentesting)
- Accompanying and supporting internal and external acceptance procedures
- Targeted audit of ISMS and other compliance requirements
- Managed Security Services for a continuous monitoring of objects of investigation and re-testing of new releases and features
- Optional confirmation of the security level of objects of investigation by a corresponding TÜViT certificate

For our services we take into account procedures and audit criteria with regard to threat scenarios of national and international standards and best practices (e.g. OWASP[1], WASC[2], CESG[3] and BSI[4]).

The second chapter presents the TÜViT competencies, followed by our service catalog for the Cyber Security Services field of application. Chapter 3 next describes typical test and audit criteria and also an example penetration test process. Additional information on boundary conditions and about TÜViT is summarized in Chapters 0 and 5, followed by the contact data of the contact persons in Chapter 6.

[1] The Open Web Application Security Project
[2] The Web Application Security Consortium
[3] The National Technical Authority for Information Assurance
[4] Federal Office for Information Security

2 Competencies

Conformity confirmations with regard to compliance requirements are an essential requirement in the case of security-relevant IT products and IT systems. Corresponding certificates are central criteria for order placements or approvals by authorities. As a member of the Alliance for Cyber Security and as a recognized test center of the Federal Office for Information Security (BSI), TÜViT tests, confirms and certifies the IT conformity of various different objects of investigation.

Alliance for Cyber Security

TÜViT participates in the Alliance for Cyber Security as a partner and thus proves its competence in the area of Cyber Security. In addition to free information events and webinars, TÜViT also supports – apart from small and medium-sized companies – also large industrial companies when building cyber security awareness and offers fully comprehensive measures for protection against cybercrime threats from a single source.

Figure 1: Partner logo of the Alliance for Cyber Security

Certified IT Security Service Provider

As a TÜV NORD GROUP company, TÜViT has numerous test centers, which are also internationally recognized and accredited, in the area of IT Quality Assurance, IT Security and Data Protection.

TÜViT has been certified by the German Federal Office for Information Security as an IT Security Service Provider in the field of IS Revision and IS Consulting as well as Penetration testing (Certificate Number: BSI-APS-9006) and has BSI-certified penetration testers as well as IS auditors and consultants.

Figure 1: BSI logo for certified IT-Security Service Providers

2.1 Specification of Services

In the cyber security field, TÜViT offers a range of different test procedures and certifications, which respectively extend across specific technologies and application areas. For testing and confirming products, services, infrastructures and complex networked solutions in the cyber environment, TÜViT has developed the test procedure

Security Qualification.

The Security Qualification, as a standardized modular test procedure, was included in the Trusted Certification Program by TÜViT as

- Trusted Site Security (TSS) for operators as well as
- Trusted Product Security (TPS) for manufacturers

and addresses in a suitable manner cross-sector application scenarios taking particularly into account the heterogeneity, complexity and dynamics to be handled as a rule.

The test criteria and the test procedure here are in line with the Tailored Assurance Service (CTAS) of the British CESG as well as the corresponding directives and best practice approaches of OWASP, WASC and the BSI.

The modular test procedure is characterized by a systematic engineering way of proceeding and always comprises penetration tests which offer a significantly higher flexibility than, for example, the processing of formal checklists. The Security Qualification is suitable for examining a large number of test objects from relatively simple individual components to highly complex networked cyber solutions for very different application scenarios. These range across technologies from simple products via Internet services and IT infrastructures to complex networked mobile solutions.

In addition to the test procedure for the Security Qualification, all test and consultation services can also be offered in the form of a

Security Analysis

which is not accompanied by the issue of a certificate. The Security Analysis was conceived as a flexible test procedure and, due to the non-standardized analysis depth, cannot be certified.

The high degree of flexibility of the Security Analysis allows TÜViT to provide various different test and consultation services in the cyber security environment with maximum individual choice. In order to ensure a continuously high security level of the objects to be examined, the so-called services can also be commissioned in the form of a Managed Security Service with the following characteristics.

- Monitoring

  TÜViT collects relevant attack vectors for the object to be examined or the respective application scenario and re-tests these within the contractual term at regular intervals.

- Re-Testing

  If required, TÜViT tests future adaptations and new features of the object to be examined.

The more sensitive the data processed and the specific application scenarios are, the higher is the attractiveness for any attackers from cyber space.

The protection and the identification of secure cyber solutions become an ever greater challenge for organizations and end users.

The **advantages of the Cyber Security Services** by TÜViT can be summarized as follows.

- Modular testing and consultation by an independent third party
- Comprehensible identification of vulnerabilities
- Objective determination of the security level
- Reliable identification of critical spheres of activity
- Project-related and continuous support
- Guidance for decision-makers and managers
- Provision of verification to supervisory institutions
- Competitive advantage due to the TÜViT certificate

3 Penetration Test Process

This chapter provides an overview of the penetration test process within the cyber security services field of application. Exemplary ways of proceeding are described as well as possible test aspects.

Subsequently, a fictitious target as well as a typical project process of a penetration test are presented.

3.1 Classification of penetration tests

Essentially a penetration test can be summarized by the following criteria:

- information basis made available
- aggressiveness level used
- scope of the object to be examined and examination depth
- procedure during the execution of the test,
- access, channel and
- starting point for the test execution (see Figure 2).

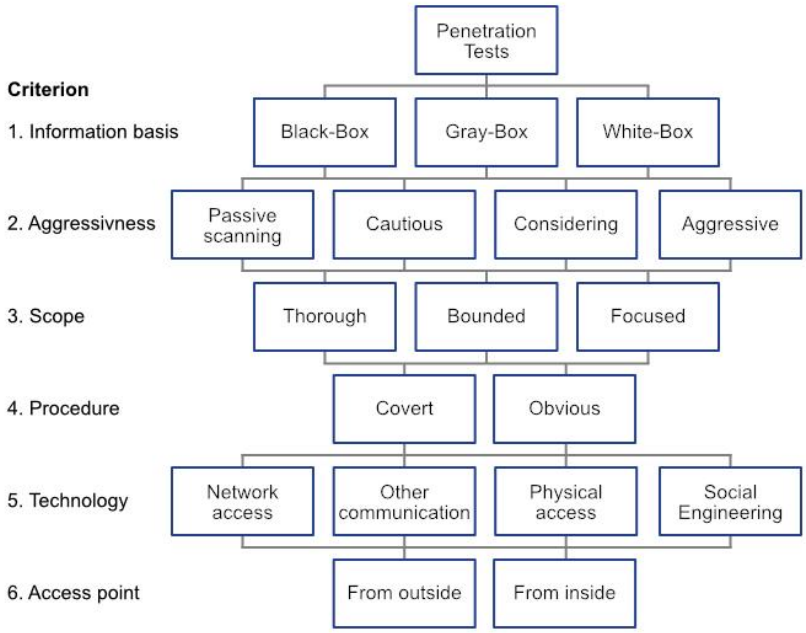

Figure 2: Classification of penetration tests
(source: penetration test execution concept by the BSI)

3.2 Procedure and Analysis Depth

Depending on the individual client requirements and the service selected, TÜViT - by way of example - can offer the following test activities.

3.2.1 Documentation Analysis

This test method provides for a review of the documentation (e.g. with regard to architecture, use and administration). Accordingly, the analysis will examine operating and system documents which describe the behavior and the properties of systems and components (e.g. installation manuals, configuration guides and maintenance instructions).

3.2.2 Inspections on Site

For examining the IT infrastructure, on-site inspections are carried out in the data center. The on-site inspections focus on the access restrictions to the data centers, server rooms and operating premises, as well as systems and components of the test object.

3.2.3 Interviewing Responsible Persons

This test method provides for interviews with persons having responsibilities with regard to security-relevant processes, functions and tasks in connection with the test object. In these interviews, persons responsible from the areas of IT Security and Administration are questioned about security-relevant aspects.

3.2.4 Configuration Analysis

This test method provides for manual configuration analyses of systems and components with the support of the persons in charge. The configuration analyses are carried out jointly with those persons. This requires unrestricted access to systems and components. In connection with the configuration analyses security-relevant and possibly also functional configuration settings must be reviewed.

Here, in the field of network and application security, essentially technical measures for system hardening, patch management, routing, logging, monitoring and, if necessary, cluster and virtualization solutions are examined and analyzed. In the area of mobile security these are essentially aspects for Mobile Device Management (MDM), Mobile Application Management (MAM) and Mobile Content Management (MCM). This test method can frequently be combined with interviewing the corresponding persons.

3.2.5 Penetration Tests at Network and System Level

This test method provides for the tool-supported verification, at network and system level, of known vulnerabilities of the systems and components to be analyzed. Here, the measurement and test platforms used by TÜViT must be integrated into the respective network segment or VLAN. IP address allocation for the measurement and test platforms is effected statically or dynamically. Depending on the test scenario, this test method essentially uses the following test activities.

- ARP scans within network segments

  This test method provides for tool-supported ARP scans within a network segment (broadcast domain). The objective of the ARP scans is the determination of all systems and components of a network segment. In order to carry out ARP scans or ping sweeps, physical access to the network level of the relevant network segment is necessary. In connection with the ARP scan or ping sweep, ARP requests or various different ICMP requests are sent out actively at network level.

- Port scans against systems and components

  This test method provides for tool-supported connection-oriented (TCP) and, if necessary, connectionless (UDP) port scans against systems and components. The objective of the port scans is host detection with OS fingerprinting, service detection and version detection. Accordingly, active scan techniques are used, which may have an effect on the system availability.

  In order to execute port scans, access to the Internet and to the network level of the relevant network segment is necessary.

  In connection with the port scans or script scans, TCP-SYN packages are actively sent at network level.

- Vulnerability scans against systems and components

  This test method provides for tool-supported vulnerability scans against systems and components. The objective of the vulnerability scans is the detection of generally known vulnerabilities in the systems and components. In order to execute vulnerabilities scans, access to the Internet and to the network level of the relevant network segment is necessary. For example, in connection with the vulnerability scans and by agreement with the person's responsible, denial of service attack vectors are also tested.

- Network sniffing within network segments

  This test method provides for the reading of network traffic within a particular network segment. In order to carry out network sniffing, physical access to the network level of the relevant network segment is necessary. For network sniffing, by agreement with the persons responsible, a man-in-the-middle attack is initially carried out, e.g. in a switched network environment, in order to determine sensitive information from the re-routed network traffic. Alternatively, the operator provides a monitoring port at the switch.

3.2.6 Penetration Tests at (Web) Application Level

This test method provides for the tool-supported verification of known vulnerabilities of the systems and components to be analyzed at application level (including web services). Here, the measurement and test platforms used by TÜViT access the applications to be analyzed via the Internet/Intranet. The necessary access data such as e.g. user name and password for the applications are made available to TÜViT for the duration of any such testing.

It must be ensured here that the number of user accounts and clients made available is sufficient. With this test method, the test activities applied essentially analyze the following aspects:

- Authentication

  This aspect is used to verify that access data are set up and used securely.

- Session Management

  This aspect is used to verify that HTTP requests, responses, sessions, cookies, headers and logging are used such that secure session management is ensured.

- Access Control

  This aspect is intended to verify access controls. Here, it is analyzed whether access protection is securely implemented in the application.

- Input Validation

  This aspect is used to verify that inputs are validated such that these can be safely used within the application.

- Output Encoding/Escaping

  This aspect is aimed at the application's output encoding and escaping. Here, it is analyzed whether the application outputs are encoded securely for external applications.

- Cryptography

  This aspect is intended to verify crypto algorithms. Here, mechanisms and algorithms for encoding, code management, random number generation and check sum operations are analyzed.

- Error Handling and Logging

  This aspect is used to verify error handling and logging. Here, it is analyzed to what extent security-relevant events are detected and attacks identified.

- Data Protection

  This aspect focuses on data security. Here, it is analyzed to what extent sensitive data (e.g. credit card data, passport or identification card numbers) are protected.

- Communication Security

  In connection with communication security, the security level of all communication processes is analyzed.

- HTTP Security

  This aspect is used to verify the security level of HTTP requests, responses, sessions, cookies, headers and logging.

- Business Logic

  This aspect is used to verify the business logic in order to analyze an unforeseen use.

3.2.7 Penetration Tests in the Enterprise Mobility Management (EMM) Environment

In order to evaluate the security of network infrastructures with externally integrated mobile end devices, it is necessary for the analysis to also include the respective mobile devices such as smartphones and tablets. For this purpose, TÜViT must be provided in almost all cases with appropriately provisioned devices. The handover of fully set up devices (Apple/Google/Mail-Account, VPN, SharePoint server, etc.) should, if possible, be effected as early as the day of the kick-off meeting.

The above-mentioned tests at network and application level use information from the weakness analysis of the mobile end devices. Furthermore, in addition to the test aspects mentioned below, the above-mentioned architecture and design criteria of the mobile solutions as well as organizational and procedural aspects are also taken into account.

- Mobile Device Management (MDM)

  This aspect is used to verify that the MDM used or the directives are correctly configured, the device settings are enforced and meet security requirements.

- Mobile Application Management (MAM)

  This aspect is used to verify that an MAM used is correctly configured and that the user can only install and use those apps that meet the directives.

- Mobile Content Management (MCM)

  This aspect is used to verify that business data stored on the device, such as documents, can leave the device only via the interfaces provided for this purpose. In addition, it will be checked whether the data can be processed only by the components provided for this purpose in accordance with any directives set up.

- Container and BYOD/COPE solutions

  In contrast to the “security-related isolation” of mobile end devices by means of MDM, it is also standard – particularly in connection with many BYOD and COPE regulations – that many apps and data are only available in separate security-related areas, so-called containers. This test aspect is directed against apps and data within the container as well as against the container itself in order to review the protection targets required.

- Data loss prevention

  Particularly in the case of mobile devices used professionally, it is important to prevent any data loss due to loss, user ignorance, damaged apps as well as various different attack methods. Frequently, this aspect represents a combination of several other test aspects listed here.

- Remote Wipe

  This aspect covers the remote wipe of the devices and analyzes to what extent this has been implemented effectively.

- Jailbreak/Rooting Detection

  Container and MDM solutions frequently enforce that higher user privileges are detected so as to protect defined data against unauthorized access. This test aspect checks the effectiveness of the technical detection mechanisms and procedural measures.

- Data access control

  This aspect covers the device registration / log-in of the user, the PIN for example. It is checked whether access controls can be circumvented and how the actual specific implementation is to be evaluated from a security-related point of view.

- Encryption

  Data to be protected should be stored in encrypted form, particularly on mobile devices. This test aspect evaluates whether and how data are persisted in encrypted form. In addition, this test aspect attempts to circumvent this encryption.

3.2.8 Analyses of Mobile Apps

In addition to the verification of mobile devices, individual applications - so-called apps - are also analyzed in terms of security. Here, depending on the issue at hand, various different dynamic and static program analysis methods are applied. In some application cases, an app has been adapted to the respective mobile end device to such a depth that it is advisable for project implementation to provide TÜViT with an appropriately provisioned device. The following test aspects cover typical issues to be analyzed with regard to app security in the Enterprise Mobility environment (EMM) or the Mobile Application Management (MAM).

- Secure data transmission

  In contrast to the above aspect, this focuses on the data transmission by the app. It is verified a.o. whether the data are correctly encrypted during transmission, for example by means of TLS, and whether any certificates involved are checked correctly.

- Authentication

  This test aspect verifies the protection mechanism of the app against any unauthorized access, for example access protection by a PIN or a similar method.

- Data loss prevention

  In addition to data loss due to theft or loss of the device or any unauthorized access to the same, such a loss can also arise from malicious or poorly programmed apps. This aspect helps to analyze the app data flow and checks how the data “leave” the app or are “forwarded”.

- Weakness analysis

  This aspect covers the robustness of the app in relation to various different attack scenarios such as SECURITY QUALIFICATIONL injection or input validation. These tests are to ensure that, if at all possible, there are no security-relevant vulnerabilities in the app to be tested.

- Source code analysis

  In source code analysis, an app is subjected to an in-depth analysis. Here, for example, (security-relevant) program routines are analyzed at source code level.

- Data protection

  In addition to technical tests, the terms of use (general terms and conditions) of an app can also be reviewed with regard to data protection aspects.

3.2.9 Advanced Persistent Threats (APT Scenarios)

In addition to the aforementioned test and consultation activities, which can be carried out either covertly or openly, depending on the classification of penetration tests, enquiries with regard to highly individual attack scenarios are increasing. This chapter summarizes exemplary APT scenarios for selected objects of investigation. In deviation from the subsequently presented APT scenarios additional attack techniques and objects of investigation are possible.

- Phishing/Spear Phishing

  In this social engineering scenario, TÜViT carries out general or targeted phishing attacks and provides as a result optionally an anonymized, statistical or personalized evaluation of success. During the same, only active call-ups or executions by the phishing mails can be collected or active and pursuing attack attempts by an attack server controlled by TÜViT can be executed in the Internet.

- Bad Devices

  In the grounds and the premises of the client, specially prepared devices will be placed as “forgotten” or “unknown” devices. This test scenario evaluates, for example, how many USB sticks are introduced by employees into the IT infrastructure or whether any unauthorized network technology is used. This verifies to what extent established organizational and technical security measures can be circumvented. As a result TÜViT supplies optionally an anonymized, statistical or personalized evaluation of the test success.

- Data Loss Prevention (DLP)

  In connection with this scenario TÜViT is given access to the IT infrastructure, for example, by the provision of a fully established standard client system including user identification. From an employee's point of view, it is then attempted to achieve unauthorized access to the Internet and unauthorized leakage/draining of data. This verifies the effectiveness of the security measures at the local systems as well as those for the central IT infrastructure.

  In this regard, for example, local attack tools as well as Internet attack servers controlled by TÜViT are used for the unauthorized data leakage.

3.2.10 Penetration Tests in the Industrial Control System (ICS) Environment

To analyze the security of automation solutions for the control of technical processes (SCADA/PLS), it is necessary to take into account also the underlying hierarchy of business processes, the communication processes and components used (e.g. HMI, BUB and ABK). In this connection TÜViT reviews organizational and technical risks at various different ICS levels (e.g. production management, operational management, process management).

- Organizational risks

  Within this risk area, organizational vulnerabilities such as insufficient degrees of documentation and IT security regulations in the form of directives and processes are evaluated. Here, the security level of remote maintenance access points and established standard IT components as well as the availability requirements of communication networks and their monitoring are assessed.

- Technical risks

  The risk potential on the basis of human error and intentional attacks is assessed at device level, network level and application level. The degree of networking and the protection of the ICS networks as well as incorrect configurations and insufficient backups of components are reviewed here. Regarding this risk area, in particular attack techniques from the previous chapters on penetration tests are applied.

3.3 Summary

The following table summarizes the above-mentioned test activities with their prerequisites and the degree of support required.

Brief description	Prerequisites	Degree of Support
Documentation analysis	Access to (internal) documentation	moderate
Inspections on site	Access and entry to the IT infrastructure	high
Interviewing persons responsible	Access to employees	high
Configuration analyses of systems and components	Access to administrators and component configurations	high
Penetration tests at network level	Access to the network level	moderate
Penetration tests at application level	Access to the application	moderate
Penetration tests in the EMM environment	Access to mobile devices/infrastructure/services/ solutions	high
Analysis of mobile apps	Access to compiled app and source code	moderate
Advanced Persistent Threats (APT)	Project-specific	moderate
Penetration tests in the ICS environment	Access and entry to the IT infrastructure and network access	high

Table 1: Test activities and methods

3.4 Example Objectives

There is a wide range of motivations for the execution of cyber security projects and penetration tests by an independent third party. The following list of example objectives therefore does not claim to be complete as the objectives may vary significantly from client to client.

- Identification of vulnerabilities (technical, organizational, procedural)
- Listing and prioritization of recommendations for action and security measures (technical, organizational, procedural)
- Increasing the security of data, systems and applications
- Increasing the effective security level of technical, organizational and procedural measures or the mixture of measures
- Increasing the security awareness of employees of all hierarchy levels (awareness)
- Preparation for an internal or external inspection and acceptance procedure or certification
- Verification of the security level by means of a corresponding certificate / seal of quality as proof of trust in relation to supervisory institutions and customers

3.5 Example Project Sequence

Starting from the many varied forms and test activities of a penetration test, the following figure outlines the classic project sequence.

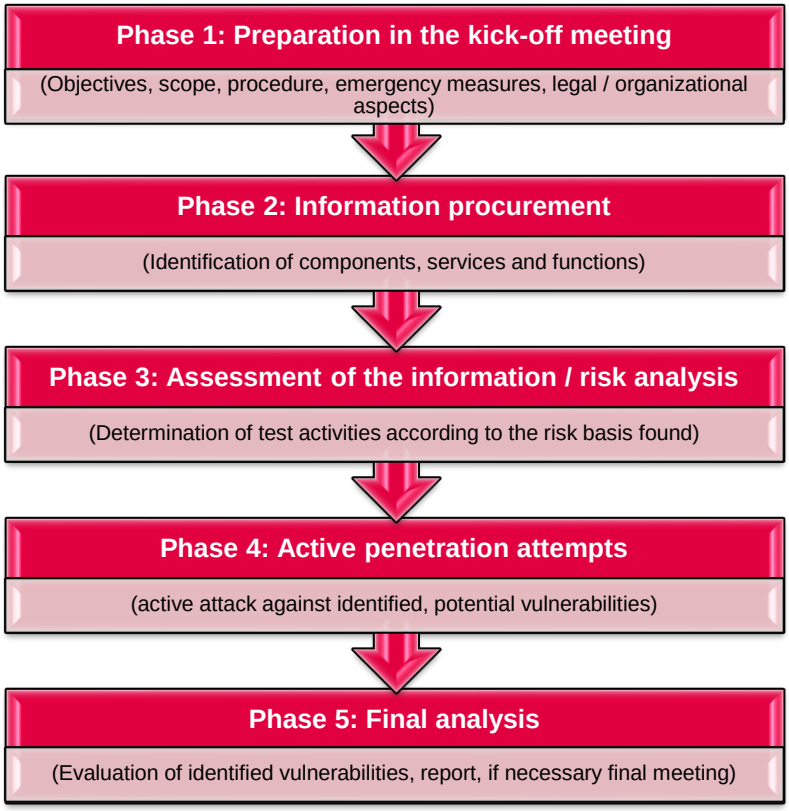

Figure 3: Example project sequence

4 Boundary Conditions

This chapter describes the boundary conditions for the preparation of quotations and for project implementation.

4.1 Information Processing for the Preparation of Quotations

For the preparation of quotations, TÜViT must be provided essentially with the following information.

- Client (company name, division/department, address, etc.)
- Contact person (for technical and organizational aspects)
- Objective and scope of the penetration test
- Examination depth and procedure for test execution
- Object to be examined
  - Network diagram, overview of architecture and design
  - Protection required for the data processed and business processes
  - Complexity of the object to be examined (e.g. role and authorization concept)
  - Technologies used for the object to be examined
  - Number of the examination object components to be tested
- Test times and place of execution
- Participation of third parties (e.g. suppliers/service providers, providers, data center operators, etc.)

4.2 Preparation for Test Execution

During test execution TÜViT partially depends on support by the client. In particular, the following prerequisites shall be met by the client.

- Accept the offer (incl. liability limitations & hacker paragraphs)
- Make available the object to be examined (incl. test accounts, mobile end devices, etc.)

4.3 Lead Time and Project Implementation

TÜViT is significantly subject to the time and project specifications stipulated by its clients. Based on experience, a project can be commenced within 2 - 4 weeks after receipt of order.

5 About TÜViT

TÜV Informationstechnik GmbH – in short **TÜViT** – with headquarters in Essen, is one of the leading providers of testing and evaluation for IT security and IT quality. By means of testing and certification, we support manufacturers, operators and users of IT systems, IT products and IT infrastructures in maintaining their corporate values.

Our experts in the area of IT security concentrate on themes such as Common Criteria Evaluation, Cyber Security, Mobile Security, Industrial Security, penetration tests, assessment of information security management systems against ISO/IEC 27001 and also data protection audits. A further aspect is testing and certification of data centers with regard to their physical security and constant availability.

In the area of IT quality, TÜViT coordinates product, quality and risk management based on recognized standards, in order to support clients in achieving important corporate objectives.

Our services are always based on the state of technology and fulfil the highest standards of security and quality.

Numerous accreditations and certifications by national and international organizations and authorities testify to our competence and expertise in the areas of IT security and IT quality.

German Federal Office for Information Security

- Recognized according to DIN EN ISO/IEC 17025:2005 for testing against ITSEC/ITSEM/CC/CEM and also BSI-TR 03121-1, BSI-TR 03121-3, BSI-TR 03132, BSI TR-03104 and BSI TR-03105 Part 3 and Part 5
- IT-Security Service Provider in the field of IS Revision and IS Consulting and Penetration Testing
- Licensed auditors for IT-Grundschutz and ISO/IEC 27001
- Licensed auditors for De-Mail

German Accreditation Body

- Testing Laboratory for IT Quality: Competence for evaluations in the field of IT Ergonomics and IT Security, accredited according to DIN EN ISO/IEC 17025:2005
  - Evaluation Body for IT Security: Accreditation for evaluations according to ITSEC/ITSEM/CC/ISO 15408/CEM
  - Evaluation Body for IT Usability: Accreditation for evaluations according to DIN EN ISO 9241-110, DIN EN ISO 9241-11, ISO/IEC 25051, DIN EN ISO 13407 and ISO 9241-210
- Certification Body: Competence for certifications of products in the field of IT Security (ITSEC, Common Criteria, ETSI EN 319 401 / 319 411-1 / 319 411-2 / 319 421, ETSI TS 101 456 / 102 042 / 102 023, DIN EN 50518-1:2014 / -2:2014 / -3:2014), accredited according to DIN EN ISO/IEC 17065:2013
- Certification Body: Competence for certifications of products, processes and services in accordance with EN ISO/IEC 17065:2013 and ETSI EN 319 403 V2.2.2 in the scope qualified trust service providers and the qualified trust services provided by them in the scope of application REGULATION (EU) No 910/2014 (eIDAS)

German Federal Network Agency

- Confirmation Body according to Signatures Act/Signatures Ordinance for the confirmation of products for qualified electronic signatures
- Confirmation Body according to Signatures Act/Signatures Ordinance for the confirmation of the implementation of security concepts for certification service providers

German Banking Industry Committee

- Listed Testing Body for Electronic Payment Transactions

Independent Center for Privacy Protection Schleswig-Holstein

- Expert test center for IT products (legal/technical)

Information-technology Promotion Agency, Japan

- IT Security Evaluation Facility: Competence for evaluations according to CC/CEM

National Institute of Technology and Evaluation, Japan

- Evaluation Body for IT Security: Accreditation according to DIN EN ISO/IEC 17025 in the field of IT / Common Criteria evaluations (Lab Code: ASNITE0019T)

National Institute of Standards and Technology, USA National Voluntary Laboratory Accreditation Program, USA

- Evaluation Body for IT Security (NVLAP Lab Code: 200636-0) for Cryptographic Module Testing (scopes 17BCS, 17CAV/01, 17CMH1/01, 17CMH1/02, 17CMH2/01, 17CMH2/02, 17CMS1/01, 17CMS1/02, 17CMS2/01, 17CMS2/02) and Biometrics Testing

Europay, MasterCard and Visa, USA/Great Britain/Japan

- Full Service Laboratory for evaluations of ICs and IC cards according to EMVCo Security Guidelines
- Modular Label Auditor

Visa, USA

- Test House for performing Visa Chip Product security evaluations

MasterCard, Great Britain

- Accredited to perform CAST (Compliance Assessment and Security Testing) evaluations

Betaalvereniging Nederland, Netherlands

- Evaluation Laboratory

TÜViT participates actively in developing the state of the technology within national and international research projects and bodies.

TÜViT itself operates an effective quality management system and environmental management which are certificated according to ISO 9001:2008, fulfilling the high requirements and expectations of its clients.

TÜViT belongs to the **TÜV NORD GROUP,** headquartered in Hannover. TÜV NORD employs more than 10,000 employees worldwide and is, in addition to the German market, represented in 70 countries in Europe, Asia and America. In the course of the 140 years of TÜV tradition, TÜV NORD has performed and developed tests and assessments in very many areas. Based on its fundamental principles, TÜV NORD GROUP is obliged to offer and perform its services on an independent and neutral basis.

6 Contact

Dennis Schröder, M. Sc.

Produktmanager Cyber Security Services

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstrasse 20
45141 Essen, Germany

Phone: +49 201 8999-606
Fax: +49 201 8999-666
d.schroeder@tuvit.de
www.tuvit.de