eicar

THE CRIMINAL RELEVANCE OF IT SECURITY AUDITS

WAYS TO ACHIEVE LEGAL CERTAINTY IN IT SECURITY AUDITS AGAINST THE BACKGROUND OF THE NEW COMPUTER CRIMINAL LAW

by Christian Hawellek*
developed from a project work together with Dennis Jlussi*.
*candi. iur. at the Gottfried Wilhelm Leibniz University of Hanover

Content

Abstract

IT security audits are essential to grant information protection as well as data and network security. However, the legal framework, especially regarding German computerrelated criminal law – considerably extended since summer 2007 –, is anything else than trivial. While mere passive scanning for vulnerabilities alone constitutes no offence, any kind of exploitation generally meets the scope of Section 202a StGB (data espionage). Simulated DOS attacks represent a system interference in terms of Section 303b StGB, actions related to antivirus and antispy software efficiency testing may fall within the scope of Section 303a StGB (data interference). Finally the usage of any socalled „sniffer software“ – indispensable in context of securing network functionality – would constitute a classical case of data interception (Section 202b StGB). While the latter is justified due to Section 88 III 1 TKG, any of the former actions – apart from those rare cases when it would be justified as an act of necessity (such as Sections 228 BGB, 34 StGB) – will demand approval of the respective authorised person to remain legal. Authorised persons to legitimate security audits in case of companies are their legal representatives, such as the management board of a corporation, whereas this right can be delegated in terms of company organisation to single departments, too. In those few constellations, where private data on company systems is affected and the respective action is not justified, the approval of the particular employee is mandatory, if there is no corresponding employer/works council agreement. The declaration of approval should name the particular tests and their purpose, the systems to be audited and any existing risk in that context.

Introduction

Ensuring the integrity and functionality of a company's own IT systems is of fundamental importance for companies. Not only does a potential failure of information infrastructures entail considerable economic risks, but a risk management system is also legally required, at least for stock corporations, due to Section 91 II of the German Stock Corporation Act (AktG) introduced by the KonTraG. Regardless of whether the services of external providers are used or whether the company has its own CERTs and IT Security departments exist: ensuring information protection, data security, network functionality and application security is a high priority.

However, effective security checks often cannot be carried out without appropriate simulations, especially with regard to targeted attacks on the corresponding infrastructures. However, the legal situation in this regard is anything but trivial, especially with regard to computer criminal law. This was most recently demonstrated by the introduction of § 202c of the German Criminal Code was amended by the 41st Criminal Law Amendment Act in the summer of 2007 in the discussion on the question of whether the procurement of so-called hacker tools - which are indispensable for the IT security industry in order to carry out realistic audits - could possibly lead to the criminalization of the professional circles involved[1].

In fact, however, there are considerable risks of criminal liability far beyond the scope of application of Section 202c of the German Criminal Code (StGB), which are sometimes hardly perceived in practice. During comprehensive IT security audits, for example, almost all of the relevant criminal offenses of the Computer Security Act are usually investigated. criminal law. Legal admissibility here therefore therefore necessarily presupposes a flawless prior authorization in terms of scope and chain of legitimation, the requirements of which can by no means be derived from the from the law alone. Rather, in-depth knowledge of criminal law is required to precisely define the legal framework for permissible IT security checks. Especially in the case of permitted private use of IT systems by employees, the legal situation is relatively complex.

This will be taken as an opportunity to briefly present the criminal offenses relevant to IT security checks and to examine the common test actions with regard to their relevance under criminal law. Finally, it will be shown how legal certainty can be achieved in practice by means of a legally flawless authority and how to design it.

[1] See Jlussi, "IT-Sicherheit und § 202c StGB," EICAR Position Paper, http://www.eicar.org/press/infomaterial/JLUSSI_LEITFADEN_web.pdf; Jlussi/Hawellek, "IT-Sicherheit im Lichte des Strafrechts" for a detailed account.

B. The individual offenses

Computer criminal law was introduced into the German Criminal Code in 1986 with the 2nd Act to Combat Economic Crime[2] and modified and supplemented by the 41st Criminal Law Amendment Act[3] in summer 2007. The penal norms relevant in the context of IT security audits are found in two different sections of the StGB. Section 15 "Violation of personal privacy and secrecy" contains those criminal offenses that make unauthorized access to information a punishable offense - Section 202a of the Criminal Code (spying on data), Section 202b of the Criminal Code (interception of data) and Section 202c of the Criminal Code (preparation of spying on and interception of data). In turn, the criminal liability for manipulating data and IT systems has been expanded in Section 27 "Damage to Property" by inserting the criminal offenses of data alteration and interception. (§ 303a StGB) and computer sabotage (§ 303b StGB) have been regulated.

I. § 202a StGB - Data Espionage

§ 202a StGB - Spying on data

(1) Whoever, without being authorised to do so, obtains access, by circumventing the access protection, for themselves or another, to data which were not intended for them and were specially protected against unauthorised access incurs a penalty of imprisonment for a term not exceeding three years or a fine.

According to Section 202a of the German Criminal Code (StGB), it is a criminal offense to gain access to third party data if it is specially secured against this and this security is circumvented. The offense was created in 1986 to close the gap in criminal liability that existed at the time with regard to the "hacking" of information systems. The act is a crime of success, the mere attempt remains unpunished. Since information protection is one of the main goals of IT security audits, this criminal standard is by far the most frequently affected. What is new since summer 2007 is that the data no longer has to be actually accessed, but that the mere possibility of doing so is sufficient, which has considerably expanded the scope of criminal liability.

In the context examined here, "data" means all electronically coded information in information systems,[4] regardless of how marginal the information content may be.[5] "Access" means at least the possibility of retrieval. It is irrelevant whether the data is stored or in the process of being transmitted, so that the interception and decryption of messages is also covered.[6]

The characteristic feature of the criminal offense is the overcoming of access protection, which is intended to protect the authorized party from unauthorized access to the data and to document his interest in secrecy.[7] Data that is generally accessible anyway - such as website content with only a "secret" URL - cannot therefore be spied out in a way that constitutes an offense. Access protection includes all types of access barriers, for example passport word barriers or RFID access cards, as well as the Encryption of otherwise freely accessible data.

[2] 2nd Act to Combat Economic Crime, BGBl. 1986 I p. 72.
[3] 41st Criminal Law Amendment Act, BGBl. 2007 I p.1786.
[4] 2nd WiKG-E, BT-Drucks. 10/5058, p. 29; MünchKomm-Graf, § 202a Rn. 7f.; Sch/Sch-Lenckner, § 202a Rn. 3.
[5] MüchKomm-Graf, § 202a marginal no. 8ff.
[6] 2nd WiKG-E, BT-Drucks. 10/5058, p. 29; MünchKomm-Graf, § 202a para. 10.
[7] 2nd WiKG-E, BT-Drucks. 10/5058, p. 29; MünchKomm-Graf, § 202a marginal no. 28; Sch/Sch-Lenckner, § 202a marginal no. 7.

B. The Individual Offenses

If a file that is not protected against downloading but is encrypted is loaded from a server and the encryption is then bypassed or otherwise removed, this is also covered.[8]

Of particular importance for the admissibility of IT security checks is the question of the destination of the data. If access takes place with the consent of the authorized user, the data is no longer "not intended for the perpetrator "[9] , so that the existence of the crime and thus criminal liability no longer apply. Therefore, an IT security check on behalf of the authorized person is permissible despite the use of otherwise punishable methods.

With the creation of Section 202b of the German Criminal Code (StGB) as part of the 41st Criminal Code Amendment Act in summer 2007, the criminal liability gap regarding the interception of unencrypted data, which is not covered by Section 202a of the StGB, was closed. The scope of protection differs from that of Section 202a of the Criminal Code in that it does not depend on the existence of special access protection, i.e., the right to "non-publicity of communications "[10] is protected in general. In the area of IT security, the standard primarily plays a role in the use of so-called "sniffer" software, such as that used by is used for maintenance and troubleshooting in IP networks.

II. § 202b StGB - Phishing

§ 202b - Phishing

Whoever, without being authorised to do so, intercepts data (section 202a (2)) which are not intended for them, either for themselves or another, by technical means from non-public data transmission or from an electromagnetic broadcast from a data processing facility incurs a penalty of imprisonment for a term not exceeding two years or a fine, unless the offence is subject to a more severe penalty under other provisions.

III. § 303a StGB - Data manipulation

§ 303a - Data manipulation

(1) Whoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) incurs a penalty of imprisonment for a term not exceeding two years or a fine.

(2) The attempt is punishable.

(3) Section 202c shall apply mutatis mutandis to the preparation of an offense pursuant to paragraph 1.

[8] Sch/Sch-Lenckner, § 202a marginal no. 8.
[9] 41st StrÄndG-E, BT-Drucks. 16/3656, S. 9.
[10] 41st StrÄndG-E, BT-Drucks. 16/3656, S. 11.

B. The Individual Offenses

The criminal offense of "data manipulation" (Section 303a of the Criminal Code) protects the right to the intact usability of the information stored in the data against any form of alteration, including the withdrawal of the data or the destruction of the information content.[11] In contrast to Section 202a of the German Criminal Code (StGB), there is no special protection against unauthorized modification. With regard to IT security checks, the standard usually plays a role when viruses or Trojans are used to test the performance of corresponding defense software and data such as registry entries are changed as a result. It also plays a role when insecure passwords are changed and data is blocked as a result. With regard to Section 303a of the German Criminal Code (StGB), the consent of the person authorized to dispose of the data also leads to exemption from punishment, since the unlawfulness ceases to apply with the justifying consent.

IV. § 303b StGB - Computer sabotage

§ 303b - Computer sabotage

(1) Whoever interferes with data processing operations which are of substantial importance to another by

1. committing an offence under section 303a (1),

2. entering or transmitting data (section 202a (2)) with the intention of adversely affecting another or

[...]

incurs a penalty of imprisonment for a term not exceeding three years or a fine.

[...]

The object of protection under Section 303b of the German Criminal Code (StGB) is the owner's interest in the uninterrupted flow of data processing on his information systems,[12] the corresponding disruption must be of a significance that exceeds an impairment that can be remedied with little (financial, temporal, etc.) effort - a mere threat is not sufficient for this purpose[13] The 41st Criminal Law Amendment Act supplements the criminal offense of computer sabotage in that DOS attacks are now also explicitly punishable under No. 2, which is somewhat cryptically worded.[14]

In the context of IT security audits, the standard tends to play a subordinate role, since such aggressive tests are not generally carried out. If this should nevertheless be the case, the first two cases standardized by law are usually relevant. These are, on the one hand, data modification under Section 303a of the German Criminal Code (StGB), if it has correspondingly serious consequences (such as the overwriting of a boot sector by a test virus), and, on the other hand, DOS attacks, if they cause serious disruption, constitute an act punishable under Section 303b of the StGB. In both cases, the consent of the person in whose property the information system is located also excludes criminal liability at the justification level, although the authority to do so must

[11] Sch/Sch-Stree, § 303a marginal no. 1.
[12] Sch/Sch-Stree, § 303b marginal no. 1.
[13] Resolution recommendation of the Legal Affairs Committee on the 2nd WiKG-E, BT-Drucks. 10/5058, S. 35.
[14] This follows from the explanatory memorandum, 41st StrafÄndG-E, BT-Drucks 16/3656, p. 13.

B. The Individual Offenses

be granted after sufficient prior information about possible consequences due to the high risk involved. However, if only separate test systems set up for this purpose are subjected to corresponding checks, the elements of § 303b of the German Criminal Code (StGB) are usually already excluded for lack of justification.
The data processing carried out there does not fulfill the requirement of "essential importance", so that criminal liability does not apply for this reason Alone.

C. IT security audits in practice and their relevance under criminal law

I. Information gathering via "hacker forums" and similar sources

Gathering information about vulnerabilities in software and how to exploit them is upstream of IT security audits and is one of the daily tasks of a CERT, being able to counter new potential dangers with the shortest possible reaction times. The search for such information does not constitute a criminal offense, regardless of the source used. Criminal liability always begins with the (unauthorized) actual exploitation of vulnerabilities.

II. "Honeypots" as attack targets

Larger companies often have their own IT security departments that are responsible for protecting the IT infrastructure. Since IT security is to be ensured in a known and largely static technical environment, it makes sense to set up honeypots, i.e., information systems that serve the sole purpose of being the target of an attack. This method allows real attacks to be "captured" and analyzed in terms of the attacker's modus operandi and persona. The setting up of such systems does not constitute a criminal act, nor does it constitute incitement to commit a criminal act.

C. IT security audits in practice and their relevance under criminal law

III. Use of scanner software for vulnerability analysis

Most IT security checks start with the use of scanner software for vulnerability analysis, such as AppScan, GFI Languard or Nessus. Data is sent to the scanned system in order to detect open ports and other vulnerabilities and to draw conclusions about the software in use from the system's reaction (the "signature"). Although the performance of these passive scans leads to the transmission of data from the scanned system, this is exclusively information that is logically located before any existing access protection and is therefore not itself protected against access. Section 202a of the German Criminal Code is therefore not applicable to purely passive scans. In the rare cases in which the scan should, contrary to expectations, lead to a system crash of the scanned system, such a crash was not intentionally caused, so that a possible criminal liability according to Section 303b I No. 2 is also ruled out. Passive scans are therefore permissible under criminal law.

IV.The exploitation of vulnerabilities

In some cases, scanner software - such as AppScan - offers the possibility of exploiting vulnerabilities found after the scanning process, in order to further investigate the vulnerability of the checked system. This can be done by using own or third-party exploits. In principle, the scope of application of Section 202a of the German Criminal Code (StGB) is affected, but the cases of exploiting security vulnerabilities or trap doors deliberately built in by the software creator are legally controversial. Such a procedure could be regarded as access without overcoming access protection, because there is no such protection with regard to the gap. However, since the information system as a whole is to be taken into account, the exploitation of hidden gaps is precisely the overcoming of the security measures in place for regular access.[15] Section 202a of the German Criminal Code (StGB) therefore remains applicable.

If only test systems are attacked, criminal liability does not apply as a rule, since the attacker and the subject of the legal interest are identical or the provision of the test system for this purpose already implies the consent of the authorized party. If productive systems such as web servers are attacked, criminal liability is only excluded if the action is covered by the consent of the legal owner. The same applies if access to a protected network or terminal is gained by IP spoofing or session hijacking[16] or - even if only to a limited extent - by SQL injections or cross-site scripting.

V. Password cracks and use of Trojan software

The successful overcoming of password locks classically falls within the scope of Section 202a of the German Criminal Code (StGB),

[15] MünchKomm-Graf, § 202a marginal no. 66.
[16] MünchKomm-Graf, § 202a marginal no. 72.

C. IT security audits in practice and their relevance under criminal law

if this enables access to protected data and systems. It is irrelevant whether the password is obtained by manual testing, a brute force attack or a dictionary attack. If cracking the password also requires data from the system, e.g. hash values, which must first be obtained and then calculated back to the plaintext by means of rainbow tables, the reading of the hash value is punishable, provided that the hash value is also protected against access. If this is not the case, the punishability starts as with all other password cracks only with the successful overcoming of the password lock. If the data of an RFID access card is decrypted, this already constitutes a criminal offense without the need to actually use a counterfeit RFID card with this data.

The spying on passwords or other data by means of Trojan software is punishable as soon as this access is obtained, if access to a protected system is required for its installation. If the Trojan is introduced into the system in another way, for example by deceiving the user into installing it, the criminal liability begins at the moment when the possibility of transmitting protected data exists. If the Trojan software also alters data such as registry entries in the infected system, then the offence of Section 303a of the German Criminal Code (StGB) is fulfilled.

All of the aforementioned procedures are therefore only permissible insofar as they are carried out in agreement with the respective legal entity.

VI. Changing insecure passwords

If insecure passwords are discovered during the password security check - for example, those that are preset in the hardware at the factory - they usually have to be changed for security reasons.
The storage of private data falls as blocking of data within the scope of Section 303a of the German Criminal Code (StGB), and must therefore be agreed with the responsible departments within the company. If employees are also permitted to store private data on company computers - which is rather seldom the case in practice - it must be remembered that they themselves are legal entities with regard to their private data. Although the changing of insecure passwords, if the corresponding employee cannot be identified in time and there is a corresponding potential danger for the legal interests of the company, justified as an act of necessity, the employee nevertheless, the person concerned should be informed as soon as possible.

VII. Use of virus software

To check the functionality and performance of defense programs, it may be necessary to use existing or self-written viruses. The use of such software usually falls within the scope of Section 303a StGB. Such a procedure is permissible on test systems that are prepared or set up for this purpose.

C. IT security audits in practice and their relevance under criminal law

Production systems in use during the test could also be subjected to such tests after sufficient information about the risks involved and subsequent explicit permission, but this rarely seems necessary in view of the risks involved. The programming of viruses, for example with virus construction kits, is not punishable under Section 202c in conjunction with Section 303a III of the German Criminal Code (StGB) if they are used solely for testing purposes under the above-mentioned conditions (and this is ideally also documented) and the virus software is not passed on to third parties.[17]

VIII. Use of "sniffers" to ensure network security

To ensure network functionality and to analyze attacks, it may be necessary to monitor network traffic with sniffers and to view individual IP packets. However, the use of sniffers is software is a classic application of Section 202b of the German Criminal Code. In this context, it is problematic that the person authorized to dispose of the acquired data cannot be determined in advance, since it is not possible to foresee whose data will be intercepted. Permission based on prior approval is therefore out of the question here; criminal law does not recognize subsequent approval in the sense of civil law. However, the question arises as to what happens with thesniffer software if it is used exclusively to secure the functionality of telecommunications networks and is indispensable for this purpose. In this case, at least the secrecy of telecommunications would not be affected due to the concretization in § 88 III 1 TKG. The relationship between Section 202b of the German Criminal Code (StGB) and Section 88 of the Telecommunications Act (TKG) has not yet been examined by legal scholars. However, there is no apparent reason why the non-public nature of communications should be protected beyond the scope of telecommunications secrecy. In particular, it would be contrary to purpose to take the measures required for network security first by Section 88 III 1 TKG, in order to then make it punishable again via Section 202b of the German Criminal Code (StGB). In this respect, the use of sniffer software, insofar as it is indispensable for the secure operation of the telecommunications network, is justified under Section 88 III 1 TKG and thus not punishable.

[17] Jlussi, "IT-Sicherheit und § 202c StGB," EICAR Position Paper, p. 12, http://www.eicar.org/press/infomaterial/JLUSSI_LEITFADEN_web.pdf; Jlussi/Hawellek, "IT-Sicherheit im Lichte des Strafrechts," p. 69.

[18] Telecommunications Act, Federal Law Gazette I p. 1190, as last amended by Article 2 of the Act of December 21, 2007, Federal Law Gazette I p. 3198.

D. Legal requirements for the declaration of consent

I. Determination of the legal entities

In accordance with the description just given, the vast majority of IT security checks are only permissible if the relevant activities have previously been authorized to the extent they have been carried out by the legal entity. The determination of the legal owner varies depending on the direction of protection of the relevant criminal law. In addition, in certain cases, a distinction must be made between data relating to the company that employees store on company computers in the course of their work (company data) and data that employees store privately (private data).

1. Personal Scope of Protection of § 202a StGB

The object of protection under Section 202a of the German Criminal Code (StGB) is the so-called formal right of disposal[19] over the data, i.e. the right to access the intellectual content of the stored information. This does not take into account the ownership of the data carrier used[20] and - although the systematic position of the norm would suggest - the personal confidentiality area[21]. Thus, the protection of the norm is not enjoyed by the person to whom the data refers[22] - as is the case in data protection law - but by the person who has the right to decide on access to the data.[23] If, for example, personal data of employees is stored in leased information systems of the employer, only the employer itself is protected with regard to a hacking of these systems, but not, for example, the lessor as the owner of the systems or the employee whose data was read out. The latter, in turn, is adequately protected under criminal law by the special provisions of Sections 43 and 44 of the German Federal Data Protection Act (BDSG), which sanction violations of data protection law.[24] Thus, a person who is entitled to access data and who documents his or her interest in secrecy by means of access protection is a person who is legally protected within the meaning of Section 202a of the German Criminal Code (StGB).

a) Company data

With regard to company data, access protection within the framework of information protection protects the formal confidentiality interest of the company in its data against access by unauthorized persons inside and outside the company. It does not matter who actually installs this access protection or who stores the protected data. Rather, it is relevant on whose behalf this is done and who is authorized to make decisions regarding access to the information.[25] Therefore, with regard to the authority to dispose of company data, it is irrelevant that the employee uses a personal password known only to him/her and that the protected data was entered by him. Rather, the employee merely fulfills his or her obligation to complete the protection provided by the access security measures set up by the company. The company alone is therefore the legal owner of the company data.

[19] SK-Hoyer, § 202a marginal note 1, Sch/Sch-Lenckner, § 202a marginal note 1, Lackner/Kühl, § 202a marginal note 1, LK-Schünemann, § 202a marginal note 2.
[20] MünchKomm-Graf, § 202a marginal no. 17; Weißgerber, NZA 2003, 1005-1009 [1007].
[21] 2nd WiKG-E, BT-Drucks. 10/5058, S. 28.
[22] Sch/Sch-Lenckner, § 202a marginal no. 1.
[23] SK-Hoyer, § 202a marginal no. 1; LK-Schünemann, § 202a marginal no. 2, Sch/Sch-Lenckner, § 202a marginal no. 1.
[24] Sch/Sch-Lenckner, § 202a marginal no. 1.
[25] BayObLG v. 24.06.1993 - 5 St RR 5/93; MünchKomm-Graf, § 202a StGB Rn. 17.

D. Legal requirements for the declaration of consent

b) Private Data

However, if private use of the hardware provided by the company is permitted to a certain extent, the question arises as to who is authorized to dispose of the resulting private data. This already becomes relevant if no private data may be stored on the data storage media, but this data is automatically generated during permitted private Internet use, for example as browser history or cookies. This case constellation is legally controversial and has not yet been conclusively clarified.

Here too, however, the decisive question is who expresses his or her interest in secrecy in these data by setting up access protection. Since the employee may not install any additional access protection on the information system used by him, he cannot document a confidentiality interest vis-à-vis the company in a legally permissible manner. Instead, the employee enjoys the protection provided by the access security measures installed by the company anyway. However, this does not make these access protections the employee's own, since the employee cannot influence their existence, their properties and the question of who else has access to the system. In particular, the employee is aware that while he himself may not make data on his computer accessible to anyone else, the company may very well allow other employees - for example administrators - access via their passwords. Ultimately, it is the sole decision of the company which employee should have has access to which equipment or not.

Private data stored on the information systems in a permissible manner thus lacks a special access protection that would manifest the employee's formal interest in secrecy precisely vis-à-vis the company.[26] According to the opinion expressed here, a separate declaration of consent by the employee concerned is therefore not required even for IT security checks that allow access to privately stored data.

This result by no means leaves the employee unprotected, since Section 202a of the German Criminal Code is only intended to protect the formal authority to dispose of data, but not the personal confidentiality of the person to whom the data relates. The latter, in turn, enjoys sufficient protection under §§ 43, 44 BDSG. The employer or or a third party commissioned by him may access the employee's employee's private data, insofar as this data is related to a person in the sense of § 3 I BDSG, only by asserting by asserting overriding legitimate interests pursuant to § 28 I No. 2 BDSG and may only and only inspect them to the extent necessary for this purpose. If such legitimate interests, which also include the security and functionality of the information systems, are present, an encroachment on the employee's personal secrecy is permissible under data protection law. Against this background, it seems all the more unconvincing to construct an encroachment on the employee's formal interest in secrecy in order to carry out an IT security check via the detour of the Section 202a of the German Criminal Code (StGB).

Nevertheless, this view is not uncontroversial in legal scientific community.[27]

[26] Barton, CR 2003, 842.
[27] For example, Weißgerber, NZA 2003, 1007, on the protection of private employee data under criminal law.

D. Legal requirements for the declaration of consent

Legal certainty, even according to the contrary view, can only be achieved if, in the case of permitted private use, the consent of the employees concerned to the respective IT security checks is also available. If inhouse IT security departments are active, a corresponding company agreement could be worked towards, for example as part of the company agreement that regulates the private use of company resources such as PCs and Internet access.

2. Personal scope of protection of the sections 202b, 303a, 303b StGB

Personally protected by Section 202b of the German Criminal Code (StGB) is the person who is authorized to dispose of the intercepted data. However, it is impossible to determine this in advance in the practical cases of the use of sniffer software, as it is not possible to predict whose data will be intercepted by chance. However, the interception of data is permissible in accordance with the above description, insofar as it is necessary to ensure network functionality and security, on the basis of the justification in Section 88 III 1 TKG, so that in these cases it is not necessary to obtain the consent of the person entitled to the intercepted data, insofar as the executor is actually legally entrusted with ensuring network functionality.

The legal owner of company data within the meaning of Section 303a of the German Criminal Code (StGB) is also the company. Here, too, the employee, even if he or she has created the data, is not himself or herself the subject of legal protection, since ultimately only the company has the right to determine whether data should be changed, deleted or blocked. However, if private data is stored on the company's information systems, it may usually only be changed with the employee's consent. Exceptions to this are only made in cases where the change is justified - for example, due to a state of emergency - such as in the described cases of changing insecure passwords.

Section 303b of the German Criminal Code (StGB) protects the owner of the information systems in terms of personnel, i.e., the company in this context. Since test systems are not covered by this provision due to the lack of significant data processing, in practice, consent is only required for attacks against production systems, namely DOS attacks against servers. It should be noted here that effective consent presupposes corresponding knowledge of the consequences, so that it is essential to provide complete and correct information.

II. Further requirement for the consent form

1. Person of the permittee

If the company is the sole legal owner, IT security audits are permitted by its legal representatives, such as the managing director of a GmbH (§ 35 I GmbHG) or the executive board of a stock corporation (§ 78 I AktG). However, the right to do so can be delegated to subordinate bodies of the company management within the framework of the company organization[28], in

[28] MünchKomm-Graf, § 202a marginal no. 18.

D. Legal requirements for the declaration of consent

these cases, the responsible employees of the relevant departments can also legally authorize IT security audits. In the rare cases in which the legal interests of employees are also affected and there is no justifiable reason, such as an emergency, their consent must be obtained unless an company agreements exist in this regard.

2. Individual agreement or general regulation

IT security audits can be permitted on an individual, concrete basis in individual cases or on a general, abstract basis by means of internal company regulations. The former is appropriate when external service providers are used or the group's own IT security departments carry out security audits in legally independent subsidiaries. In both cases, tests are usually only carried out for a certain period in a manageable number. Here, it can be individually regulated in advance which checks are to be carried out using which methods.

If, on the other hand, regular IT security checks are to be performed by the company's own CERT, for example, these can also be generally permitted within the company's internal rules and regulations. This is practically a two-step process. First, the company management, which in principle has the sole authority to permit such audits, will delegate this right to a subordinate body so as not to be burdened with it itself.

It must therefore be regulated within the company that a specific department may determine the permissibility and scope of IT security audits and is expressly authorized by the company's management to permit interventions in the corresponding legal assets protected by criminal law to the extent deemed necessary. In the second stage, this department then draws up regulations for the performance of IT security audits that describe the procedures and scope in detail. These can be adapted unproblematically according to requirements and technical developments; entire classes of checks (such as tests of all web servers for application security) can also be permitted as a whole, provided that this is formulated in a sufficiently precise and delimitable manner. It is also possible to allow additional one-off tests that are not otherwise permitted under the rules, for example if a running web server is to be checked for DOS security as an exception.

3. Time and form of authority

In terms of criminal law, a distinction is made in legal doctrine between consent that precludes the commission of an offense (e.g., in § 202a StGB) and justifiable consent (e.g., in §§ 303a, 303b StGB). of the legal owner. While the former only needs to be actually present, the latter must always be explicitly declared prior to the execution of the act. In view of the legal security of the verifier, however, it is advisable in both cases to ensure that a corresponding authorization is fixed in writing before the test begins. In this way, evidentiary difficulties such as civil liability risks can also be avoided.

D. Legal requirements for the declaration of consent

4. Content of the declaration of consent

The declaration of consent should initially contain the tests to be performed and their objectives, because these are essential characteristics of the scope of the intervention permitted in each case. In cases of doubt, the planned procedure should also be specified if this is not already clear from the first two points. Furthermore, the systems to be checked must be clearly delimited to ensure that no tests are carried out that are not covered by the authorization. Insofar as there are risks that systems under test will fail or otherwise be disrupted - even and especially if this is not the intention of the test - their nature and hazard potential must be explained, unless only separate test systems are affected. Such risks should be mentioned in the consent form, at least in bullet points, in order to avoid evidentiary difficulties with regard to the scope of the explanation. Finally, as far as possible, it should be ensured that the permitting person is actually authorized to do so, if this is not already evident from his or her function in the company to be audited. In general, the greater the risk and the more intensive the encroachment on the protected legal asset, the higher the requirements for prior clarification and the level of detail of the corresponding declaration of consent. As long as this is taken into account, IT security checks can be carried out without any risk of criminal liability.