TeleTrusT
Pioneers in IT security.

(Neu-)Entdeckung des „Stands der Technik“

Der „Stand der Technik“ als vermeintlich „neue“ Erfindung der aktuellen Gesetzgebung bringt Unternehmen in die schwierige Lage, etwas zu erfüllen, was nicht hinreichend definiert ist. Was jedoch nicht konkret definiert ist, bietet viel Raum für Interpretationen. Im Streitfall wird die Rechtsprechung entscheiden, ob das geforderte Sicherheitsniveau eingehalten wurde. Unternehmen können jedoch vorsorgen und sich mit dem Thema rechtzeitig auseinandersetzen.

Von Tomasz Lawicki, Associated Senior Auditor bei der Sachverständigen-Sozietät Dr. Schwerhoff und Leiter des Arbeitskreises „Stand der Technik“ beim TeleTrusT – Bundesverband IT-Sicherheit e. V.

In den vergangenen zwei Jahren hat der Begriff „Stand der Technik“ durch die Gesetzgebung an Brisanz gewonnen: Aus dem IT-Sicherheitsgesetz (IT-SiG) resultiert die Verpflichtung zur Einhaltung des Stands der Technik augenscheinlich nur für die Betreiber kritischer Infrastrukturen (KRITIS-Betreiber) sowie mittelbar auch für ihre IT-Dienstleister – „augenscheinlich“, da auch die Anbieter von Telemediendiensten durch das angepasste Telemediengesetz (TMG) zur Berücksichtigung des Stands der Technik verpflichtet wurden. Mit dem Kabinettsbeschluss vom 25. Januar 2017 zur Umsetzung der Europäischen Richtlinie zur Gewährleistung hoher Netz- und Informationssicherheit (NIS-RL) rücken die Anbieter von so genannten „Digitalen Diensten“ stärker in den Fokus (vgl. www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/01/nis-umsetzungsgesetz.html). Auch die im Sommer 2016 veröffentlichte Europäische Datenschutz-Grundverordnung (DS-GVO) fordert die Berücksichtigung des „Stands der Technik“ (siehe http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679).

Alle diese gesetzlichen Änderungen führen dazu, dass sich alle Unternehmen mit der Bestimmung, der Einhaltung und dem Nachweis des „Stands der Technik“ ihrer technischen und organisatorischen Maßnahmen auseinandersetzen müssen.

Begrifflichkeit

Der Begriff „Stand der Technik“ ist nicht gänzlich neu: In vielen Bereichen der Gesetzgebung ist er schon längst verankert und wird regelmäßig in öffentlichen oder privaten Ausschreibungen sowie in Verträgen seit Langem verwendet. Neu ist jedoch, dass die Einhaltung oder mindestens die Berücksichtigung des „Stands der Technik“ der technischen und organisatorischen Maßnahmen in Verbindung mit der IT-Sicherheit und dem Datenschutz gesetzlich vorgegeben ist und bei festgestellten Verstößen sehr hohe Strafen drohen.

Und damit beginnt schon die mehrschichtige Problematik, wenn es darum geht, das geforderte Sicherheitsniveau, also den „Stand der Technik“, einzuhalten oder nachzuweisen. Der Gesetzgeber fordert zwar den „Stand der Technik“, nennt jedoch keine Kriterien zu seiner Bestimmung. Was jedoch nicht konkret definiert ist, kann nicht bewertet und auch nicht eingehalten werden. Erschwerend kommt hinzu, dass die gesetzlichen Vorgaben aus IT-SiG und DS-GVO nicht aufeinander abgestimmt sind. Für einen CIO ist es von daher schwierig, die konkreten Maßnahmen am gesetzlich geforderten „Stand der Technik“ praxistauglich zu bestimmen und nachhaltig auszurichten.

Die Bestimmung des „Stands der Technik“ ist komplex: Entgegen der in vielen Debatten vertretenen Meinung reicht es nicht aus, die Software-Patches einer Sicherheitsmaßnahme regelmäßig zu installieren, um das geforderte Sicherheitsniveau nachzuweisen. Es müssen mehrere Aspekte betrachtet werden.

„Stand der Technik“ muss dabei von den begrifflich ähnlich lautenden Technologieständen wie den „allgemein anerkannten Regeln der Technik“ und dem „Stand der Wissenschaft und Forschung“ sprachlich und messbar abgegrenzt werden. Diese drei Technologiestände lassen sich aus der „Drei-Stufen-Theorie“ der Kalkar-Entscheidung des Bundesverfassungsgerichts ableiten (BVerfGE, 49, 89 135 f).

Einfach ausgedrückt: Der „Stand der Technik“ ist innovativer als die „allgemein anerkannten Regeln der Technik“ und veralteter gegenüber dem „Stand der Wissenschaft und Forschung“. Diese Unterscheidung ist die wesentliche Grundlage für die Bestimmung des geforderten Sicherheitsniveaus. Wie viele Beispiele aus der Praxis zeigen, werden diese drei Begriffe gleichermaßen in der Rechtsprechung und in der Öffentlichkeit vermischt oder gar verwechselt (vgl. www.dthg.de/resources/Definition-Stand-der-Technik.pdf).

Ausgehend vom gewollten Zweck der Gesetzgebung werden mit dem „Stand der Technik“ ein hohes Sicherheitsniveau und hoher Datenschutz mittels fortschrittlicher Verfahren angestrebt. Implementierte Sicherheitsmaßnahmen müssen daher regelmäßig hinsichtlich ihrer Wirksamkeit im Hinblick auf die geforderten Schutzziele, ihrer Aktualität sowie ihres Innovationsgrads untersucht werden. Daraus resultiert auch ein Vergleich der Sicherheitsmaßnahmen gegen die am Markt vorhandenen Sicherheitsprodukte: Denn was heute als „Stand der Technik“ gilt, kann vielleicht schon morgen aufgrund der „innovationsbedingten Verschiebung“, also der vermeidbaren „Alterung“ der Sicherheitsmaßnahme, eher den „allgemein anerkannten Regeln der Technik“ zugeordnet werden.

Um die implementierten oder die geplanten Sicherheitsmaßnahmen einzuordnen, bedarf es einer transparenten Methodik mit eindeutigen und nachvollziehbaren Kriterien. Diese Methodik muss ermöglichen, die Sicherheitsmaßnahmen objektiv zu bewerten, sie mit Alternativen zu vergleichen und zu Nachweiszwecken zu dokumentieren. Bei der Bewertung muss neben der einzelnen Sicherheitsmaßnahme (vertikale Betrachtung) auch die Gesamtheit der Maßnahmen entlang der Datenströme untersucht werden (horizontale Betrachtung).

Basis

Als Grundlage der Bewertung können die vom BSI erarbeiteten technischen Richtlinien oder Branchenstandards (B3S) dienen. Aber auch hier gilt es genau hinzuschauen, ob die dort definierten Standards auch dem „Stand der Technik“ entsprechen: Normen und Standards neigen zur Alterung und können nur eingeschränkt als Referenz zur Einhaltung des geforderten Sicherheitsniveaus verwendet werden. Ausgehend von der zuvor erwähnten „Drei-Stufen-Theorie“ wären sie die geeigneten Kandidaten für die Kategorie „allgemein anerkannte Regeln der Technik“ und entsprechen daher nicht dem gewollten Zweck der Gesetzgebung.

Praxisnäher ist die vom Arbeitskreis „Stand der Technik“, TeleTrusT – Bundesverband IT-Sicherheit e. V. herausgegebene „Handreichung zum Stand der Technik im Sinne des IT-Sicherheitsgesetzes“, die auf einige BSI-Richtlinien verweist (www.teletrust.de/publikationen/broschueren/stand-der-technik/). Das Dokument betrachtet in erster Linie die Vorgaben aus dem IT-SiG und liefert einige Beispiele zum „Stand der Technik“ aus den Bereichen „Vernetzung“, „Internetzugang“, „Digital Enterprise Security“, „Client- und Serversicherheit“, „Mobile Security“ sowie den dabei relevanten Prozessen. Die technischen Grundlagen, die sich aus der DS-GVO ergeben, befinden sich derzeit in Erarbeitung.

Fazit

Unternehmen wird geraten, sich mit dem „Stand der Technik“ im Zusammenhang mit dem IT-SiG und der DS-GVO frühzeitig zu beschäftigen, um unternehmensweite Strategien am geforderten Sicherheitsniveau nachhaltig auszurichten. Angesichts der schnell vorübergehenden Übergangsfristen für die Umsetzung der gesetzlichen Vorgaben sowie der stetig wachsenden Bedrohung durch Cyber-Kriminalität bleibt nicht allzu viel Zeit.

Hersteller sind aufgefordert, Unternehmen aktiv zu unterstützen und innovative Sicherheitsprodukte anzubieten, die nach den Prinzipien „Security by Design“ und „Privacy by Design“ ausgerichtet sind und eine modulare, unternehmensspezifische Einhaltung der Vorgaben aus dem IT-SiG und der DS-GVO ermöglichen. ■

TeleTrusT-Gremien

TeleTrusT-AG „Biometrie“
Leiter: *Prof. Dr. Christoph Busch,* Fraunhofer IGD
Stellvertretender Leiter: *Alexander Nouak,* Fraunhofer IGD, und Georg Hasse, secunet

TeleTrusT-AG „Blockchain“
Leiter: *Dr. Andrè Kudra,* esatus

TeleTrusT-AG „Cloud Security“
Leiter: *Oliver Dehning,* Hornetsecurity

TeleTrusT-AG „Forum elektronische Vertrauensdienste AK A“
Leiter: *Christian Seegebarth,* Bundesdruckerei
Stellvertretender Leiter: *Clemens Wanko,* TüViT

TeleTrusT-AG „Gesundheitstelematik“
Leiter: *Dr. Christoph F.-J. Goetz,* KVB

TeleTrusT-AG „IT Security made in Germany“
Leiter: *Thorsten Urbanski,* G Data

TeleTrusT-AG „ISM“
Leiter: *Werner Wüpper,* WMC Wüpper Management Consulting

TeleTrusT-AG „IT-Sicherheit in der Marktforschung“
Leiter: *Erich Wiegand,* ADM Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e. V.

TeleTrusT-AG „Mobile Security“
Leiter: *Patrick Michaelis,* The Auditing Company, Sachverständigen-Sozietät Dr. Schwerhoff
Stellvertretender Leiter: *Ronny Kaminski,* Sama Partners

TeleTrusT- AG „Politik“
Leiter: *Oliver Dehning,* Hornetsecurity

TeleTrusT-AG „Recht“
Leiter: *RA Karsten U. Bartels,* LL.M., HK2 Rechtsanwälte
Stellvertretender Leiter: *RA Dr. Axel von dem Bussche,* TaylorWessing

Arbeitskreis „Stand der Technik“
Leiter: *Tomasz Lawicki,* The Auditing Company, Sachverständigen-Sozietät Dr. Schwerhoff

TeleTrusT-AG „Smart Grids/Industrial Security“
Leiter: *Steffen Heyde,* secunet

TeleTrusT-AG „SOA Security“
Leiter: *Dr. Bruno Quint,* Corisecio

TeleTrusT-AG „SICCT“
Leiter: *Jürgen Atrott,* TüViT

Arbeitsgruppe „Technik“ der TeleTrusT-EBCA
Leiter: *Henrik Koy,* Deutsche Bank

TeleTrusT-Projekt „TeleTrusT European Bridge Certificate Authority“ (EBCA)
Sprecher des Lenkungsgremiums: *Markus Wichmann,* Siemens

TeleTrusT-Projekt „TeleTrusT Information Security Professional“ (T.I.S.P.)
Sprecherin des Boards: *Birgitte Baardseth,* isits AG International School of IT Security

TeleTrusT-Projekt „Certified Professional for Secure Software Engineering“ (T.P.S.S.E.)
Sprecherin des Boards: *Petra Barzin,* secorvo security consulting

TeleTrusT-Projekt „Cyber Security Challenge Germany“ (CSCG)
Projektkoordinatoren: *Marieke Petersohn* und *Martin Fuhrmann,* TeleTrusT

TeleTrusT-Initiative „IT Security made in Germany“ (ITSMIG)
https://www.teletrust.de/itsmig/

TeleTrusT-Anbieterverzeichnis IT-Sicherheit
https://www.teletrust.de/anbieterverzeichnis/

TeleTrusT – Bundesverband IT-Sicherheit e. V.

Der IT-Sicherheitsverband

Der Bundesverband IT-Sicherheit e.V. *(TeleTrusT)* ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert *TeleTrusT* den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. *TeleTrusT* bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. *TeleTrusT* ist Träger der „*TeleTrusT* European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate „*TeleTrusT* Information Security Professional" (T.I.S.P.) und „*TeleTrusT* Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens „IT Security made in Germany". *TeleTrusT* ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Vorstand

Vorsitzender
Prof. Dr. Norbert Pohlmann
Institut für Internet-Sicherheit if(is)
Westfälische Hochschule
Neidenburger Straße 43
45877 Gelsenkirchen

Stellvertreter
Dr. Rainer Baumgart
secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen

Beisitzer
Ammar Alkassar
Rohde & Schwarz Cybersecurity GmbH
Mühldorfstraße 15
81671 München

RA Karsten U. Bartels, LL.M.
HK2 Rechtsanwälte
Hausvogteiplatz 11A
10117 Berlin

Kommunikation

Pressekontakt
Dr. Holger Mühlbauer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 40054306
holger.muehlbauer@teletrust.de

Geschäftsführung

Dr. Holger Mühlbauer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 40054306
holger.muehlbauer@teletrust.de

Bundesgeschäftsstelle

Marieke Petersohn
Projektkoordinatorin
marieke.petersohn@teletrust.de

Martin Fuhrmann
Projektkoordinator
martin.fuhrmann@teletrust.de

Marion Gutsell
Assistentin
marion.gutsell@teletrust.de

Vi Linh Tran-Graef
Assistentin
vilinh.tran-graef@teletrust.de

Ida Köhler
Projektassistentin
ida.koehler@teletrust.de

Regionalstellen

TeleTrusT-Regionalstelle Hamburg
c/o WMC GmbH
Ellen Wüpper
Zimmerstraße 1
22085 Hamburg
Tel.: +49 40 6503360
info@wmc-direkt.de

TeleTrusT-Regionalstelle Kiel
c/o 8ack GmbH
Björn Christiansen
Werftbahnstraße 8
24143 Kiel
Tel.: +49 431 55683481
office@8ack.de

Regionalstellen

TeleTrusT-Regionalstelle Bremen
c/o OTARIS Interactive Services GmbH
Mehmet Kus
Fahrenheitstraße 7
28359 Bremen
Tel.: +49 421 68511100
teletrust@otaris.de

TeleTrusT-Regionalstelle Düsseldorf
c/o exceet Secure Solutions AG
Christian Schmitz
Rethelstraße 47
40237 Düsseldorf
Tel.: +49 211 43698951
christian.schmitz@exceet.de

TeleTrusT-Regionalstelle Leipzig
c/o Rohde & Schwarz Cybersecurity GmbH
Augustusplatz 9
04109 Leipzig
Tel.: +49 341 39299343-0
info@rohde-schwarz.com

TeleTrusT-Regionalstelle Dresden
c/o T-Systems Multimedia Solutions GmbH
Oliver Nyderle
Riesaer Straße 5
01129 Dresden
Tel.: +49 351 28202680
oliver.nyderle@t-systems.com

TeleTrusT-Regionalstelle Chemnitz
c/o digitronic computersysteme gmbh
Matthias Kirchhoff
Oberfrohnaer Straße 62
09117 Chemnitz
Tel.: +49 371 81539241
mk@digitronic.net

TeleTrusT-Regionalstelle Köln
c/o FSP GmbH
Ralf Bräutigam
Albin-Köbis-Straße 8
51147 Köln
Tel.: +49 2203 3710000
info@fsp-gmbh.com

TeleTrusT-Regionalstelle Frankfurt/Main
c/o QGROUP GmbH
Thomas Blumenthal
Phoenix Haus
Berner Straße 119
60437 Frankfurt/Main
Tel.: +49 69 9050590
t.blumenthal@qgroup.de

TeleTrusT-Regionalstelle München
c/o itWatch GmbH
Ramon Mörl
Aschauer Straße 30
81549 München
Tel.: +49 89 62030100
info@itWatch.de

TeleTrusT-Regionalstelle Wien
c/o AIT Austrian Institute of Technology GmbH
Andrea Nowak
Donau-City-Straße 1
1220 Wien
Österreich
Tel.: +43 50 5500
andrea.nowak@ait.ac.at

Regionalkontakt Silicon Valley
c/o Auconet Inc.
San Francisco
USA
info@teletrust.de

Mitgliederverzeichnis

Eine aktuelle Liste der TeleTrusT-Mitglieder finden Sie online auf www.teletrust.de/ueber-teletrust/mitglieder/

TeleTrusT
Pioneers in IT security.

auf der CeBIT

c/o secunet (Halle 6, Stand J30) und c/o Rohde & Schwarz Cybersecurity (Halle 6, Stand J16)

Hannover, 20. bis 24. März 2017

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik (BSI) Halle 6, Stand H30

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde am 1. Januar 1991 gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern. Das BSI ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft. Als Behörde ist sie damit im Vergleich zu sonstigen europäischen Einrichtungen einzigartig. Derzeit sind ca. 600 Mitarbeiter mit dem Schwerpunkt Informatik, Physik und Mathematik beschäftigt. Seinen Hauptsitz hat das BSI in Bonn.

Mit der rasanten Fortentwicklung der Informationstechnik entstehen in fast allen Bereichen des Alltags neue IT-Anwendungen – und damit auch immer neue Sicherheitslücken. Je abhängiger der Mensch von der Informationstechnik wird, desto mehr stellt sich die Frage nach deren Sicherheit. Unsere Gesellschaft ist stärker als zuvor durch Computerversagen, -missbrauch oder -sabotage bedroht. Bisher kann nicht ausreichend sichergestellt werden, dass die Informationstechnik das tut, was sie soll, und nichts tut, was sie nicht soll. Weil die Probleme in der Informationstechnik so vielschichtig sind, ist auch das Aufgabenspektrum des BSI sehr komplex: Das BSI untersucht Sicherheitsrisiken bei der Anwendung der Informationstechnik und entwickelt Sicherheitsvorkehrungen. Es informiert über Risiken und Gefahren beim Einsatz der Informationstechnik und versucht Lösungen dafür zu finden. Dies beinhaltet die Prüfung und Bewertung der IT-Sicherheit von IT-Systemen, einschließlich deren Entwicklung in Kooperation mit der Industrie. Auch bei technisch sicheren Informations- und Telekommunikationssystemen können Risiken und Schäden durch unzureichende Administration und Anwendung entstehen. Um diese Risiken zu minimieren beziehungsweise zu vermeiden, wendet sich das BSI an eine Vielzahl von Zielgruppen: Es berät Hersteller, Vertreiber und Anwender von Informationstechnik. Darüber hinaus analysiert es Entwicklungen und Trends in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik

Postfach 200363
53133 Bonn
Telefon: 0228 99 9582-0
Telefax: 0228 99 9582-5400
Homepage: http://www.bsi.bund.de