FAST DETECT

SACHVERSTÄNDIGENBÜRO
FÜR IT-FORENSIK

LEITLINIE

INFORMATIONSSICHERHEIT, DATENSCHUTZ UND QUALITÄTSMANAGEMENT

UNSER UNTERNEHMENSERFOLG BASIERT AUF SICHERHEIT UND QUALITÄT

Die Leistungsschwerpunkte von FAST-DETECT umfassen die Bereiche IT-Forensik, Sicherstellungsunterstützung und Datenrettung.

Wir arbeiten jeden Tag mit äußerst sensiblen und höchstvertraulichen Informationen. Unabhängig davon, ob es sich um elektronische Daten, Akten oder Gesprächsinhalte handelt: Der angemessene Schutz dieser Informationen ist unverzichtbar für den hohen Sicherheitsanspruch und das Renommee unseres Unternehmens.

Aus diesem Grund setzen wir hochentwickelte Sicherheitstechniken ein und arbeiten auf Basis zertifizierter Abläufe. Zudem trägt jeder einzelne Mitarbeiter die Verantwortung, seinen Beitrag zur Informationssicherheit, zum Datenschutz und zur Einhaltung unseres Qualitätsniveaus zu leisten.

UNSERE PRINZIPIEN

POLIZEILICHE ÜBERPRÜFUNG VON MITARBEITERN UND RÄUMLICHKEITEN

Die IT-forensische Auswertung von Datenträgern geschieht unter hohen Sicherheitsvorkehrungen. Sie erfolgt ausschließlich durch polizeilich überprüftes und forensisch geschultes Personal.
Unsere hochgesicherten, polizeilich abgenommenen, alarm- und videoüberwachten Räume sind für Dritte unzugänglich. Dies ist eine wesentliche Voraussetzung für die Beauftragungen durch Staatsanwaltschaften und Gerichte.

SICHERHEITSZONEN

Unsere Infrastruktur ist strikt in unterschiedliche Zonen unterteilt. Das interne Netzwerk, in dem sensible Informationen verarbeitet werden, ist von außen unzugänglich.

MELDUNG VON VORFÄLLEN UND FEHLERN

Jedes Ereignis, das die Qualität, den Datenschutz oder die Sicherheit beeinträchtigen könnte und jeder Verstoß gegen Sicherheitsregeln werden gemäß unseres Incident Managements unverzüglich der verantwortlichen Stelle gemeldet. Anschließend werden die Ursachen analysiert und erforderliche Maßnahmen veranlasst.

AUFGABENBEZOGENE AUTORISIERUNG UND VIER-AUGEN-PRINZIP

Jeder Mitarbeiter verfügt nur über genau die Berechtigungen, die er benötigt, um ihm anvertraute Aufgaben zu erledigen. Diese Rechte werden regelmäßig überprüft.

Für den Abschluss bestimmter, definierter Prozesse muss zur Kontrolle eine zweite autorisierte Person die Freigabe erteilen.

RICHTLINIEN, ARBEITS- UND VERFAHRENSANWEISUNGEN

Die Umsetzung unserer Prinzipien wird in den Richtlinien sowie in den Arbeits- und Verfahrensanweisungen von FAST-DETECT definiert. Diese Dokumente legen verbindliche Vorgaben sowohl für Verhaltensweisen und Prozesse als auch für die IT-Infrastruktur fest. Für nicht spezifisch beschriebene Gegebenheiten oder Funktionalitäten werden die Regeln sinngemäß angewendet.

EIGENVERANTWORTUNG

Jeder Mitarbeiter ist für seine Handlungen verantwortlich und verpflichtet sich, sorgfältig mit sicherheitsrelevanten und personenbezogenen Informationen umzugehen sowie stets qualitätsbewusst zu agieren. Personenbezogene Daten werden nur im gesetzlich erlaubten Umfang verarbeitet.

AUDITS, KONTROLLEN UND SCHULUNGEN

FAST-DETECT überprüft regelmäßig den verantwortungsbewussten Umgang mit Prozessen und Informationssystemen innerhalb des Unternehmens. Schwerwiegende Verstöße können sowohl arbeitsrechtliche als auch strafrechtliche Konsequenzen zur Folge haben.
Interne Schulungen finden in regelmäßigem Turnus und zusätzlich bei relevanten Änderungen der Sicherheitsrichtlinien oder Qualitätsvorgaben statt.
Systematische Awareness-Maßnahmen schärfen das Sicherheitsbewusstsein bei den Mitarbeitern.

EIN AUSZUG UNSERER TECHNISCHEN UND ORGANISATORISCHEN SICHERHEITS-MASSNAHMEN

1. Regelmäßige und unangekündigte, polizeiliche Ortsbegehungen zur Abnahme der Räume, zur Überprüfung der Sicherheitsvorkehrungen und zur Überprüfung anwesender Personen.
2. Betrieb einer Klasse-C-Alarmanlage mit Wachdienst-Aufschaltung und direkter Polizei-Zuziehung, Betrieb einer Brandschutzmeldeanlage, Installation spezieller Einbruch-Hemmnisse in allen Räumlichkeiten.
3. Größtmöglicher Schutz der Asservatenkammer und der Akten-Tresore.
4. Redundante Langzeit-Video-Überwachung in den Eingangsbereichen und in allen kritischen Zonen.
5. Umsetzung eines Zonen-Sicherheitskonzepts unter anderem durch strikte physikalische Trennung des Auswertungsnetzwerkes von anderen Netzwerken und dem Internet.
6. Jährlich wiederkehrende polizeiliche Sicherheitsüberprüfung aller Mitarbeiter.
7. Limitierter und dokumentierter Akten-, Verfahrensdaten- und Beweismittelzugriff durch interne Mitarbeiter.
8. Vertragliche Verpflichtung aller Mitarbeiter mit Zugriff auf Beweismittel und Verfahrensdaten zur strikten Berücksichtigung relevanter Richtlinien und zu besonderer Verschwiegenheit.
9. Sicherer und ISO-zertifizierter Transport sowie schonender und verwechslungssicherer Umgang mit Beweismitteln und Akten.
10. Ernennung eines unternehmensinternen TÜV-zertifizierten Datenschutzbeauftragten (BDSG).

Abb. Reifegrad-Checkliste

ÜBERWACHUNG UND MESSUNG

REIFEGRADMODELL

Die Anforderungen an ein optimales Qualitätsmanagement nach ISO 9001 und Information Security Management nach ISO 27001 werden permanent mit der IST-Situation des Unternehmens abgeglichen. Hierfür kommt die von FAST-DETECT entwickelte Reifegrad-Checkliste zum Einsatz.

- Sie berücksichtigt alle aktuellen Normen.
- Sie ist an die besonderen Erfordernisse der IT-Forensik-Branche angepasst.
- Sie ist mit einem Bewertungssystem versehen und kann jederzeit Auskunft über den aktuellen Status im Unternehmen geben.

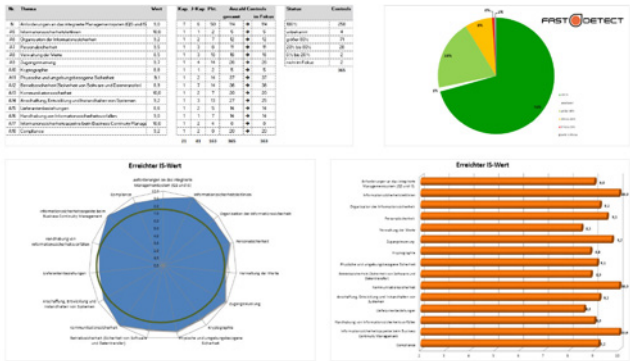

Abb. Der Grad der Übereinstimmung wird über ein Ampelsystem und über eine Werte-Skala angezeigt.

AUDIT- UND MASSNAHMENPLAN

Die Einhaltung innerbetrieblicher und normativer Anforderungen wird durch regelmäßige Audits überwacht. Alle Ergebnisse dieser Audits sind protokolliert und die erforderlichen Tätigkeiten sind im Maßnahmenplan aufgenommen. Dies ermöglicht eine zielgenaue Planung und Steuerung und stellt die kontinuierlichen Verbesserungen im Qualitäts- und Information Security Management nachvollziehbar dar.

Jährlich stattfindende, externe Audits des TÜV Süd unterstützen FAST-DETECT beim Erkennen zusätzlicher Verbesserungsmöglichkeiten.

DIE VORGABEN FÜR INFORMATIONS-SICHERHEIT UND DATENSCHUTZ

Die folgenden Vorgaben sind in den FAST-DETECT Sicherheitsstandards und im Bundesdatenschutzgesetz festgeschrieben. Sie werden unter Beachtung der geltenden gesetzlichen Bestimmungen erfüllt.

VERTRAULICHKEIT VON INFORMATIONEN

Informationen sind nur den Personen zugänglich, die zur Nutzung dieser Daten berechtigt sind.

INTEGRITÄT VON INFORMATIONEN

Informationen sind vor unbefugter oder unbeabsichtigter Verarbeitung, Änderung oder Löschung geschützt.

VERFÜGBARKEIT VON INFORMATIONEN

Informationen stehen den befugten Personen im erforderlichen Umfang zur Verfügung – am richtigen Ort und zur vereinbarten Zeit.

AUTHENTIZITÄT VON INFORMATIONEN

Die Richtigkeit und Echtheit von Informationen ist gewährleistet. Ihre Herkunft ist bekannt und nachvollziehbar.

SORGFALT IM UMGANG MIT PERSONENBEZOGENEN DATEN

Es sind stets alle technischen und organisatorischen Maßnahmen umgesetzt, um den Vorgaben des Bundesdatenschutzgesetztes zu genügen.

DATENSPARSAMKEIT UND DATENVERMEIDUNG

Diese Grundsätze geben uns vor, den Umfang der erforderlichen Datenverarbeitung so gering wie möglich zu halten.

WAS WIRD DURCH DIE ZERTIFIZIERUNG NACH ISO 27001 ERREICHT? (Auszug)

Organisation der Sicherheit

Die Unternehmensleitung unterstützt aktiv die Informationssicherheit, gibt klare und verbindliche Vorgaben und sorgt für die notwendigen organisatorischen Rahmenbedingungen.

Personalsicherheit

Die Beschäftigten verstehen ihre Verantwortlichkeiten, sind für die vorgesehenen Rollen geeignet und sind sich der besonderen Anforderungen hinsichtlich Informationssicherheit bewusst. Das Vorgehen bei ungeplanten Vorfällen ist eindeutig vorgegeben.

Verwaltung der Sachwerte und Informationen

Die Sachwerte wie auch sämtliche gespeicherten Informationen der Organisation sind identifiziert, inventarisiert und klassifiziert. Der Umgang mit ihnen (z.B. Sicherung, Löschung) ist klar definiert und angemessen.

Zugangskontrolle für Daten und Systeme

Es ist sichergestellt, dass der Zugang zu relevanten Daten, Netzen und Einrichtungen auf Befugte eingeschränkt ist. Zugänge werden überwacht und Zugriffsrechte regelmäßig überprüft.

Physische und umgebungsbezogene Sicherheit

Alle sicherheitsrelevanten Werte befinden sich in überwachten Sicherheitszonen. Der Zugang ist nur autorisierten Personen möglich. Hardware wird überwacht, geschützt und regelmäßig gewartet. Das Business Continuity Management berücksichtigt ein detailliert festgeschriebenes Vorgehen bei Störungen.

Informationsübertragung

Die Sicherheit von übertragenen Informationen – sowohl innerhalb einer Organisation als auch mit externen Stellen – ist gewährleistet. Dies wird unter anderem in den Lieferantenverträgen geregelt.

Compliance

Verstöße gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Verpflichtungen mit Bezug auf Informationssicherheit sowie Verstöße gegen jegliche Sicherheitsanforderungen werden zuverlässig vermieden.

DIE VORGABEN FÜR DAS QUALITÄTS-MANAGEMENT

Unser Qualitätsmanagement-System (QMS) berücksichtigt die Erwartungen unserer Kunden sowie die Unternehmensziele von FAST-DETECT.

KUNDENZUFRIEDENHEIT

Wir erheben, verstehen und erfüllen die Wünsche und Anforderungen unserer Kunden.

QUALITÄTSDENKEN

Alle Mitarbeiter von FAST-DETECT haben das gleiche Verständnis von Qualität und beteiligen sich aktiv am Prozess der kontinuierlichen Verbesserung.

FEHLERVERMEIDUNG

Wir nutzen effiziente Werkzeuge und auditierte Vorgehensweisen, um nicht tolerierbare Abweichungen frühzeitig zu erkennen und zu vermeiden.

KONTROLLE UND OPTIMIERUNG DES QMS

Wir prüfen in internen Audits regelmäßig die Wirksamkeit und Effizienz des QMS und stellen damit einen stetigen Optimierungsprozess sicher.

WAS WIRD DURCH DIE ZERTIFIZIERUNG NACH ISO 9001 ERREICHT? (Auszug)

Kundenorientierung

Wir sind in regelmäßigem Kontakt mit den Kunden. So werden unsere Auftraggeber über den Stand der Dienstleitungserbringung informiert und können optimal in die Entwicklung und Verbesserung von Prozessen und Unterstützungstools eingebunden werden.

Qualitätsziele

Zur Messung und steten Verbesserung des Qualitätsmanagements, sind Qualitätsziele beschrieben und publiziert. Sie werden regelmäßig überprüft und bewertet.

Auftragsabwicklung

Jeder Schritt in der Dienstleistungserbringung ist dokumentiert. Die Prozesse werden regelmäßig überprüft und weiterentwickelt.

Mitarbeiterauswahl und Beschäftigung

Die Bewerberauswahl und die Einarbeitung erfolgen nach einem standardisierten Prozess. Neue Mitarbeiter werden mit hilfreichen Informationen sowie verbindlichen Verhaltensregeln versorgt und durch die Kollegen aktiv unterstützt (z.B. durch Mentoren).

Transport von Beweismitteln

Der Transport von Beweismitteln und Verfahrenssachen erfolgt durch ein ebenso ISO 9001-zertifiziertes Transportunternehmen.

TÜV SÜD ISO 9001

ZERTIFIZIERUNGSNACHWEISE

Wir sind nach den internationalen Normen ISO 9001 (Qualitätsmanagement) und ISO 27001 (Informationssicherheit) zertifiziert und stellen uns jährlich den anspruchsvollen, externen Audits durch den TÜV Süd. Mit diesem Nachweis dokumentieren wir unsere hohen Qualitäts- und Sicherheitsstandards und machen diese messbar.

Unsere Datenschutzbestimmungen werden von einem TÜV-zertifizierten Datenschutzbeauftragten überwacht.


ZERTIFIKAT

FAST-DETECT GmbH

ISO 9001:2008


ZERTIFIKAT

FAST-DETECT GmbH

ISO/IEC 27001:2013

VERANTWORTUNGSBEREICHE

Eine hohe Informationssicherheit und ein ausgeprägtes Qualitätsbewusstsein beruhen auf der erfolgreichen Kooperation der einzelnen Akteure, deren wichtigste Zuständigkeiten hier beschrieben werden.

GESCHÄFTSLEITUNG

Die Geschäftsleitung von FAST-DETECT ist dafür verantwortlich, dass die Sicherheits-, Datenschutz- und Qualitätsregeln bei allen Arbeitsprozessen und strategischen Entscheidungen eingehalten werden.

FÜHRUNGSKRÄFTE

Führungskräfte stellen für ihren Verantwortungsbereich sicher, dass Mitarbeiter, Externe und Lieferanten die relevanten Vorgaben und Standards erfüllen. Sie sind verantwortlich dafür, dass jedem Anwender die notwendigen und korrekten Zugriffsrechte zugewiesen sind.

INFORMATION SECURITY MANAGER (ISM) UND DATENSCHUTZBEAUFTRAGTER (DS)

Der ISM und der DS sind für die Entwicklung von Sicherheits- und Datenschutzstandards zuständig und kontrollieren deren Anwendung. Sie analysieren bereichsbezogene Risiken und ergreifen Maßnahmen zur Reduzierung und Vermeidung von Risiken. Sie begleiten den Zertifizierungsprozess nach ISO 27001, schärfen das Bewusstsein der Mitarbeiter hinsichtlich Informationssicherheit und Datenschutz und beraten zu diesen Themen.

QUALITÄTSBEAUFTRAGTER (QMB)

Der QMB ist für die Umsetzung der Normforderungen nach ISO 9001 zuständig. Er trägt die Verantwortung für das Qualitätsmanagement-System und sorgt dafür, dass die Prozesse zur Einführung, Realisierung und Aufrechterhaltung des QM-Systems umgesetzt werden.

INFORMATIONSEIGENTÜMER

Für alle Arten von Informationen wird ein Eigentümer bestimmt. Dieser ist dafür verantwortlich, dass die Informationen vertraulich behandelt werden, verfügbar sind und vor unbefugter Verarbeitung geschützt werden. Außerdem ist er für die Einhaltung der Datenschutz- und Sicherheitsgrundsätze in seinem direkten Umfeld verantwortlich.

ANWENDER VON INFORMATIONEN

Alle Anwender sind gesetzlich und vertraglich zum Datenschutz und zur Wahrung der Informationssicherheit verpflichtet. Im Rahmen ihrer Tätigkeiten und Aufgaben sind sie für eine ordnungsgemäße Verarbeitung und Sicherung der ihnen zugänglichen Daten verantwortlich.

Zwischenfälle und Risiken, mit denen ein Anwender nicht umgehen kann, muss er umgehend seinem Vorgesetzten melden.

IT-LEITER UND IT-SYSTEMVERWALTER

Der IT-Leiter konzipiert und realisiert eine ISM-konforme IT-Systemlandschaft. Die IT-Systemverwalter sorgen dafür, dass die Systeme qualitätsgeprüft sind und die Sicherheits- und Datenschutzbestimmungen erfüllen.

TYPISCHE SICHERHEITSRELVANTE PROZESSE

AUSWAHL VON TRANSPORTEUREN

FAST-DETECT arbeitet mit High-Value-Valoren-Transportunternehmen zusammen, die folgende Kriterien erfüllen müssen:

- Protokollierte 1:1-Zustellungen oder (notfalls) Lagerung in speziellen videoüberwachten und verschlossenen Containern
- Nachvollziehbarkeit aller Personenübergaben
- Möglichkeit einer lückenlosen Sendungsverfolgung
- Zertifizierung nach ISO 9001

ANNAHME VON BEWEISMITTELN

Alle Beweismittel werden bei der Annahme

- auf Schäden überprüft (jeder Schaden wird fotografiert und systemseitig erfasst),
- in die kleinsten auswertbaren Einheiten zerlegt (z.B. Ausbau von Festplatten aus einem Rechner),
- mit einem fallspezifischen, leicht lesbaren und verwechslungssicheren Label versehen,
- mit einem eindeutigen, maschinenlesbaren, verwechslungssicheren Barcode versehen,
- im System dem jeweiligen Fall zugewiesen und mit wichtigen Metadaten erfasst (Referenz zum Sicherstellungsverzeichnis, Seriennummern etc.)

BEISPIEL FÜR DEN SICHEREN UMGANG MIT WICHTIGEN UNIKATEN UND VERTRAULICHEN INFORMATIONEN

Um eine zugriffsgeschützte Verpackung von Akten und Beweismitteln zu gewährleisten, stellen wir unseren Kunden spezielle Siegelbänder und fälschungssichere, nicht zerstörungsfrei ablösbare 3D-Hologramm-Siegel zur Verfügung.

Das unbemerkte Öffnen der Sendung durch unbefugte Dritte ist dadurch nicht mehr möglich.

LAGERUNG VON BEWEISMITTELN

- Beweismittel und ausgebaute Datenträger werden ausschließlich durch den Asservatenverwalter an einem vom System zugeteilten und über die ganze Projektlaufzeit beibehaltenen Lagerplatz eingelagert. Die Asservatenkammer ist speziell abgesicherten.
- Akten werden grundsätzlich in einem feuerfesten Tresor abgelegt.
- Weitere fallbezogene, nicht vertrauliche Dokumente und Hilfsdokumente werden in einer dedizierten physikalischen Fall-Mappe abgelegt.

IHR ANSPRECHPARTNER

NORBERT STILLING
Datenschutzbeauftragter

Norbert.Stilling@fast-detect.de

IHR ANSPRECHPARTNER

OLIVER AßMUS
Leiter Information Security & Quality Management

Oliver.Assmus@fast-detect.de

FAST-DETECT GmbH

Inselkammerstraße 12
82008 Unterhaching
Tel +49 89 204040-0
Fax +49 89 204040-299
Mail info@fast-detect.de
Web www.fast-detect.de

10/2018