

IKT-Minimalstandard

Messinstrument für Cybersecurity

Kaum eine Branche blieb 2022 von einem Hackerangriff verschont. Dabei gibt es bereits seit 2018 einen Schweizer Standard, der Organisationen in unserem Land vor Cyberattacken schützen sollte. Aber kontrollieren CIOs dessen Einhaltung?

→ VON CHRISTIAN FICHERA



DER AUTOR

Christian Fichera ist Senior Cyber Security Consultant bei terreActive und Leiter des Teams Audit, Risk & Compliance. Seine Abteilung verfügt über langjähriges Security-Know-how, das unter anderem auf Projekten zu Penetrationstests, Red-Team-Services und Secure Code Review für Unternehmen verschiedener Branchen in der Schweiz basiert.

→ www.security.ch

Der Minimalstandard für die Informations- und Telekommunikations-Infrastruktur (IKT) wurde vom Bundesamt für wirtschaftliche Landesversorgung BWL lanciert, um Organisationen mit kritischer Infrastruktur – aber natürlich auch allen anderen – zu helfen, ihre eigene Cybersicherheit zu stärken.

Über 100 Sicherheitsempfehlungen zielen darauf ab, die IKT-Resilienz eines Unternehmens zu verbessern. So werden beispielsweise Massnahmen aufgeführt, die den unerlaubten Zugang zu Daten und Infrastrukturen abwehren und mögliche Beschädigung oder gar Zerstörung vereiteln sollen. Die empfohlenen Massnahmen sind sowohl technischer als auch organisatorischer Natur und gliedern sich gemäss den fünf NIST-Funktionen in Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. NIST steht für die US-Behörde National Institute of Standards and Technology.

Der risikobasierte Ansatz, auf dem der Standard beruht, ermöglicht es jedem Unternehmen, ein auf seine

Grösse, Branche und Bedürfnisse angepasstes Security-Level auszuwählen und umzusetzen.

DIE HERAUSFORDERUNG

Es ist allerdings eine grosse Herausforderung, die umgesetzten Massnahmen ständig auf ihre Wirksamkeit hin zu kontrollieren und den Interessensgruppen wie Geschäftsleitung, Risikomanagern oder externen Compliance-Stellen jederzeit Informationen über den Erfüllungsgrad zur Verfügung stellen zu können.

Um Unternehmen bei dieser Herausforderung zu unterstützen, bieten verschiedene Cybersecurity-Dienstleister dedizierte Audits nach eben diesem IKT-Minimalstandard an.

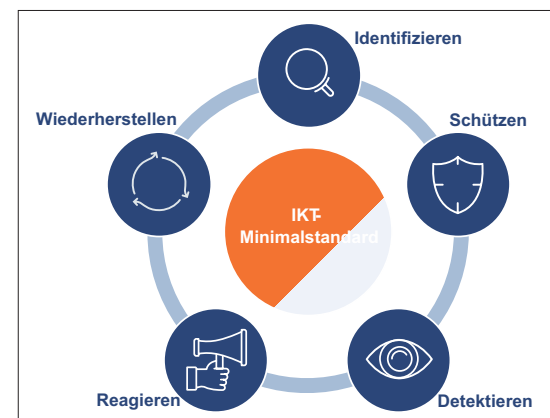
WEM DIENT EIN IKT-AUDIT?

Diese Form des IKT-Audits eignet sich einerseits für Organisationen, private Unternehmen und öffentliche Einrichtungen, die den aktuellen Reifegrad ihrer Cybersicherheit verstehen möchten. Andererseits können auch alle Organisationen davon profitieren, die ein langfristiges Projekt mit mehreren Schritten zur Verbesserung ihrer Sicherheit starten möchten.

Nun drängt sich natürlich die Frage auf, ob ein allgemeiner Standard auch universell anwendbar ist. Hier ist von Vorteil, dass der IKT-Minimalstandard unterschiedliche Maturitätsstufen aufweist. So kann jedes Unternehmen festlegen, wie hoch sein Sicherheitsbedarf ist und welche Stufe es anstrebt. Die Ziele, der Umfang der Massnahmen und das Budget können also miteinander in Einklang gebracht werden.

UMFASSENDE SECURITY-STANDORTBESTIMMUNG

Ein Audit nach IKT-Minimalstandard liefert Unternehmen eine aktuelle Security-Standortbestimmung, indem es



IKT-Minimalstandard mit NIST-Funktionen

Bild: terreActive, iStockPhoto / NicoElNino



alle Sicherheitsmassnahmen erfasst, analysiert und mit dem IKT-Minimalstandard vergleicht. Damit ist es ein effektives Instrument, mit dem ein Unternehmen durch ständige Verbesserung das angestrebte, empfohlene Sicherheitsniveau erreichen kann.

Ein solches Audit zur Sicherheitsprüfung wird typischerweise in den folgenden Schritten durchgeführt:

Bei einem Kick-Off-Meeting zwischen dem Kunden und dem externen Security-Dienstleister werden zunächst der Zeitplan und der Umfang des Audits festgelegt.

Es folgt eine Selbsteinschätzung des Kunden, der seinen eigenen Reifegrad beurteilt. Diese Phase ist nicht nur als Informationsquelle für die Analyse wertvoll, sie gibt dem Auditor auch Aufschluss darüber, inwieweit sich die Organisation der aktuellen Situation bewusst ist.

Bei der anschliessenden Analyse zieht der Security-Dienstleister die folgenden Quellen zur Auswertung heran:

- die durchgeführte Selbsteinschätzung
 - die interne Dokumentation, die der Kunde dem Auditor zur Verfügung stellt
 - die Interviews, die der Auditor vor Ort mit den verantwortlichen Mitarbeitenden des Kunden durchführt
- Abgeschlossen wird das Audit mit einem ausführlichen Bericht inklusive Massnahmenempfehlung sowie der Präsentation der Ergebnisse.

DIE WAHL DES EXTERNEN AUDITORS

Für eine erfolgreiche Projektdurchführung ist die Wahl des richtigen Auditors essenziell. Der CIO sollte daher bei der Suche verschiedene Kriterien berücksichtigen. Mehrere Jahre Audit-Erfahrung und gesammeltes Wissen aus der Zusammenarbeit mit Firmen unterschiedlicher Grösse und Branchen sind oft wichtiger als allein die Zertifizierungen (ISC2, CISA, GIAC, ISECOM usw.). Ein Auditor, der sich als technischer Spezialist auch in den Bereichen ISMS, Risk Management oder ISO 27001 weitergebildet hat, wird bei jedem IKT-Projekt einen Mehrwert liefern.

Ebenfalls von Vorteil ist ein Auditor, der neben konzeptionellen Fähigkeiten handfeste Erfahrung aus der Integration von Sicherheitskomponenten mitbringt, denn so wird er Massnahmen empfehlen, die später auch praktisch umsetzbar sind.

Wenn sich der CIO bei der Vergabe von externen Audit-Dienstleistungen bereits im Vorfeld mit den genannten Kriterien auseinandersetzt, steht einem reibungslosen Projektablauf nichts mehr im Wege.

FAZIT

Wer sein Security-Dispositiv verbessern will, benötigt zuerst einmal eine Übersicht und Analyse aller vorhandenen Massnahmen sowie eine Vergleichsmöglichkeit. Genau dies liefert das Audit nach IKT-Minimalstandard. Darauf aufbauend kann dann der Ausbau oder die Optimierung aller Security-Massnahmen beginnen. ←

Ein Audit nach IKT-Minimalstandard ist ein erster Schritt zur Verbesserung des Security-Dispositivs