ZugEstates

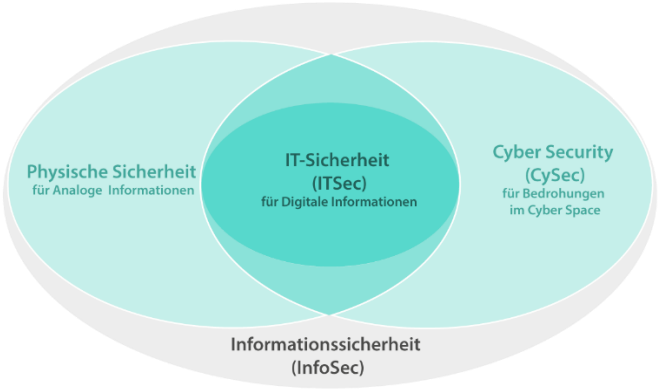
Information Security Report

Zug, 6. Januar 2025

1 Ausgangslage

Die Zug Estates Gruppe betreibt viele Initiativen mit Bezug zur Informationssicherheit, welche sich immer an den gesetzlichen Vorgaben und an «Best Practice» der Branche sowie der Unternehmensgrösse orientieren.

Mit Unterstützung von IT-Experten wurden für die ganze Zug Estates Gruppe hohe Sicherheitsstandards gesetzt, welche laufend an die aktuelle Situation angepasst werden und alle relevanten Systeme abdeckt.



1.1 Informationssicherheit (Information Security)

Die Informationssicherheit schützt alle für die Geschäftsprozesse notwendigen Daten und die datenverarbeitenden technischen Systeme mit angemessenen und wirksamen Massnahmen sowohl im technischen als auch im nicht-technischen (organisatorischen) Umfeld. Dabei folgen die risikominimierenden Massnahmen den Anforderungen der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit

1.2 Cyber Security (IT Sicherheit)

Die Themen der übergreifenden Cyber Security werden periodisch beurteilt und in konkreten Handlungsempfehlungen umgesetzt. Die festgeschriebenen Grundsätze gelten für alle Bereiche der Unternehmensgruppe und werden anhand einer Risikoeinschätzung priorisiert.

Für den Fall eines Cyber-Notfalls besteht ein Notfallhandbuch (IT Service Continuity Management). Darin sind Pflichtenhefe, Vorsorgemassnahmen, Notfallmanagement, Organisation und Kommunikation detailliert beschrieben.

1.3 Datenschutz

Der Datenschutz wird grossgeschrieben und von einem Gremium der verantwortlichen Fachbereiche periodisch aber auch im operativen Betrieb bearbeitet. Die Umsetzung des Datenschutzes orientiert sich an den gesetzlichen Vorgaben im In- und Ausland und wird unter Einbezug von Experten umgesetzt.

2 Mitarbeiterschulungen

Im Rahmen des Programms «Cyber Security Awareness» müssen alle Mitarbeitenden ein Grundwissen in den Bereichen IT-Sicherheit und Compliance erarbeiten. Dies gilt auch für neueintretende Mitarbeitende, die innerhalb von drei Monaten ein gewisses Lernniveau erreichen müssen.

Alle Lerninhalte werden zu Modulen gebündelt und sind über eine Lernplattform verfügbar. Alle Lernmodule beinhalten ein Fallbeispiel und die nötige Theorie dazu. Ein Modul gilt als abgeschlossen, sobald ein Kurztest erfolgreich absolviert wurde. Die Abteilung Digitalisierung & IT Services überwacht die Lernaktivitäten und stellt deren Absolvierung sicher. In Form von Refresher-Kursen werden Inhalte jährlich aufgefrischt.

Eine Fähigkeitsmatrix (siehe Musterbeispiel oben) zeigt dem Mitarbeitenden den Stand seines Lernfortschritts.

Nebst dem Grundwissen werden die Angestellten regelmässig mit Phishing-Simulationen geprüft. Zur Aufrechterhaltung des Wissens werden Refresher durchgeführt. Einmal im Jahr wird den Mitarbeitenden ein aktueller Fall vorgestellt, um die Sensibilisierung zu den Themen weiter zu steigern.

3 Organisation

Für die Informationssicherheit ist der Leiter Digitalisierung verantwortlich. Die Geschäftsleitung wird mehrmals und der Verwaltungsrat einmal im Jahr über den aktuellen Status der Informationssicherheit informiert.

Im Cyber Security Advisory Trust findet quartalsweise ein Austausch mit den Lieferanten statt, an dem unter anderem auch aktuelle Themen im Bereich Cyber Security besprochen werden.

Mit regelmässigen externen Sicherheitsaudits, kontinuierlichen internen Schulungsprogrammen und dem Abschluss einer Cyber Versicherung sind die notwendigen organisatorischen Massnahmen getroffen worden.

4 Sicherheitsrelevante Vorfälle

Bis jetzt gab es keine Verstösse gegen die Informationssicherheit. Der letzte sicherheitsrelevante Vorfall, ohne Datenabfluss, datiert auf das Jahr 2019. Zug Estates sind keine Datenabflüsse oder sicherheitskritischen Vorfälle bei Lieferanten oder Geschäftspartnern (Drittparteien) bekannt.

5 Assessments und Audits

Zug Estates hat 2023 im Bereich der Cyber Security ein Assessment der US-Bundesbehörde NIST (National Institute of Standards and Technology) durchgeführt[1]. Das durchgeführte Assessment erfolgte nach den Vorgaben des NIST sowie des schweizerischen IKT-Minimalstandards[2], welcher für kritische Infrastrukturen gilt. Dieses branchenunabhängige und technologieneutrale Framework dient der Identifikation von Handlungsfeldern. Es zeigt Stärken und Schwächen der eigenen IT auf und leitet konkrete Massnahmen ab.

Im Rahmen der ordentlichen Revision für das Geschäftsjahr 2023 wurde ein IT Audit durchgeführt, welches auf dem freiwilligen IT Audit von 2021 basierte, und die getroffenen Massnahmen nochmals überprüft hat.

[1] https://www.bithawk.ch/services/cyber-security-nist-assessment

[2] https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html