IT-Sicherheit
Commitment

Die vollständige Einbindung von ERP in alle Prozesse bedeutet, dass eine Beeinträchtigung oder gar ein Ausfall der Informatik grosse Auswirkungen auf die Beschaffung, auf die Produktion und die Auslieferung für die Kunden von menuandmore und damit auf deren Versorgungssicherheit hätte. Die IT-Sicherheit ist deshalb von höchster Bedeutung für menuandmore.

Beschreibung

(gemäss Management-Ansätzen plus signifikante positive wie negative Auswirkungen / Wirkungen):

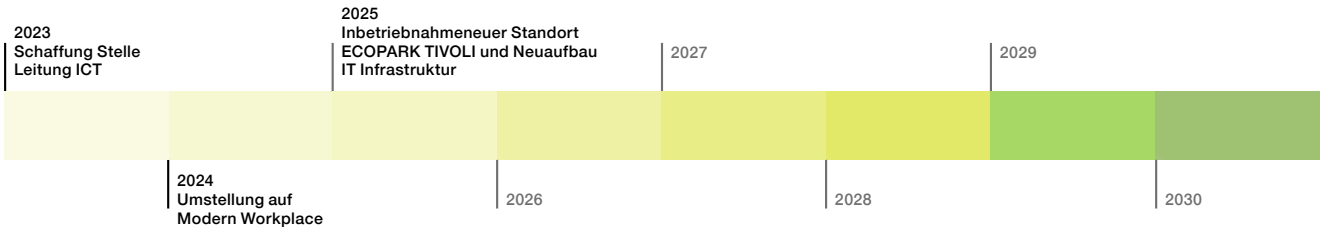
- Ein Security-Vorfall hätte zumindest temporär Auswirkungen auf die gesamten internen Prozesse (Angebotsplanung, Einkauf, Warenannahme, Produktion, Verpackung, Kommissionierung, Auslieferung)
- Beeinträchtigte IT könnte die gesamte Lieferkette (Lieferanten) stören, da keine Bestellungen getätigt werden könnten.
- Beeinträchtigte IT könnte die Kunden treffen, da sie keine Bestellungen im Webshop tätigen können.

Stand der Zielerreichungen

Ziele 2023 bis 2025	Status	Bewertung	Weiterführende Informationen
Es sind keine erfolgreichen, durch Eigenverschulden verursachten Cyber-Angriffe vorgefallen, welche einen ungeplanten Ausfall von > 1 Stunde zwischen 06:00 Uhr – 23:00 Uhr zur Folge haben.		31.12.2023: Kein Angriff mit Ausfall 31.12.2024: Kein Angriff mit Ausfall 31.12.2025: Kein Angriff mit Ausfall	• Die geplanten Massnahmen das IT-Sicherheitslevel zu überprüfen, Awareness-Schulungen durchzuführen und die ICT-Infrastruktur dem neuen Standort und aktuellen Erkenntnissen aufzubauen, wurden durchgeführt.

Ziele 2026 bis 2028	Datum	Massnahmen
Es sind keine erfolgreichen, durch Eigenschuldenverursachten Cyber-Angriffe vorgefallen, welche einen ungeplanten Ausfall von > 1 Stunde zwischen 06:00 Uhr – 23:00 Uhr zur Folge hatten	31.12.2028	• Sensibilisierung Mitarbeitende • Verbesserung des Passwort-Managements • Stärkung des Phishing-Schutzes • Einführung einer Endpoint-Detection-and-Response-Lösung (DER) • IT-Notfallplan für Cyberangriff entwickeln und testen

Wesentliche Fortschritte und Ambition bis 2030



Ambition bis 2030

Es sind keine erfolgreichen, durch Eigenverschulden verursachten, Cyber-Angriffe vorgefallen, welche einen ungeplanten Ausfall von > 1 Stunde zwischen 06:00 Uhr – 23:00 Uhr zur Folge haben

Weitere Informationen zum wesentlichen Thema der Nachhaltigkeitsberichtsperiode 2023 bis 2025; inkl. Fortschritte und Rückschritte.

Weitere Kennzahlen finden sich auf der Website von menuandmore unter:

Jahr 2023

- Im Jahr 2023 wurde eine neue Stelle für die Leitung der ICT (60 %) geschaffen und per 1. Juli besetzt.
- Es traten keine Cyber-Sicherheitsvorfälle auf.
- Parallel wurden die Vorbereitungen für das neue Datenschutzgesetz (nDSG) umgesetzt, wodurch auch die IT-Richtlinien angepasst wurden. Sie gewährleisten nun den Schutz personenbezogener Daten sowie die Einhaltung der neuen Gesetze.

Jahr 2024

- Im Frühling erfolgte die Umstellung der IT auf Modern Workplace. Für mehr IT-Sicherheit wurde zudem ein digitaler Passwortmanager eingeführt.
- Am 19. Juli 2024 gab es durch ein fehlerhaftes Update von Crowdstrike weltweite IT-Ausfälle, die einige Stunden dauerten. Betroffen war auch menuandmore. Aber der Betrieb konnte danach sofort wieder aufgenommen werden - Kunden waren also in keiner Weise beeinträchtigt. Ansonsten gab es keine Cyber-Sicherheitsvorfälle.
- Im Laufe des Jahres wurde das Pensum der Leitung ICT auf 80 % erhöht.

Jahr 2025

- Durch den Standortwechsel musste die gesamte IT-Infrastruktur neu aufgebaut werden. Dabei wurden unter anderem eine neue FortiGate 90G Firewall in Betrieb genommen, die Netzwerkverteilung redundant aufgebaut und zusätzliche Massnahmen zur Ausfallsicherheit umgesetzt. Durch den Einbau eines Moduls zur Nutzung von zwei Stromquellen kann die Netzwerkinfrastruktur bei einem Stromausfall für rund 60 bis 90 Minuten weiterbetrieben werden.
- Zusätzlich wurden die Sicherheitsleistungen erweitert. Mit der Secutec Services-Lizenzierung wurden unter anderem Secure DNS, Active Managed Threat Hunting sowie Attack Surface Management eingeführt. Dadurch können bedrohliche DNS-Anfragen blockiert, potenzielle Angriffe proaktiv erkannt und externe Angriffsflächen laufend überwacht werden. Im Rahmen dieser Sicherheitsüberprüfungen wurden auch im Darkweb veröffentlichte Zugangsdaten mit Bezug zu menuandmore festgestellt und entsprechend behandelt.
- Sämtliche Endgeräte, darunter Laptops und IoT-Geräte, wurden von einer hybriden Verwaltung auf eine Cloud-only-Verwaltung umgestellt und zentral über Mobile Device Management (Intune) verwaltet. Zudem wurde eine koordinierte Phishing-Kampagne vorbereitet und gestartet, um die Sensibilisierung der Mitarbeitenden weiter zu stärken.
- Im März 2025 kam es zu einem unautorisierten Zugriff auf ein E-Mail-Konto. Dabei wurden interne Weiterleitungsregeln erstellt und E-Mails versendet. Das Konto wurde durch die Sicherheitssoftware automatisch blockiert; anschliessend wurden aktive Sitzungen beendet, das Passwort geändert und die unautorisierten Regeln entfernt. Es entstanden keine betrieblichen Schäden.

Jahr 2026 Ausblick

- Durchführung eines externen Audit von Microsoft Tenant und somit Aufzeigen von Schwachstellen sowie Verbesserungspotential
- Erhöhung der personellen Ressourcen im IT-Team