Gut geplant in die Zukunft.

Als die Profis des Systemhauses faktordrei das digitale Equipment der H_2O Gebäudetechnik unter die Lupe nehmen, erleben sie eine Überraschung. Als dann auch noch ein Trojaner den Mailserver des Betriebs ins Visier nimmt, sind die IT-Profis mit Know-how zur Stelle.

Die H_2O Gebäudetechnik ist ein relativ junges Unternehmen „auf dynamischem Wachstumskurs". Es wurde im Jahr 2000 gegründet und deckt das komplette Leistungsspektrum der Haustechnik von Heizungen, Sanitär-, Lüftungs- und Klimaanlagen bis hin zu Lösungen mit alternativen Energiequellen ab – und das nicht nur regional, sondern sogar international. Neben der deutschen Klientel gibt es Kund*innen z. B. in Österreich, Schweden und Rumänien.

Die Nähe zum Profi wird gesucht.
Wer in solch großem Maßstab auf dem Markt tätig ist, sollte auch auf eine adäquate IT-Infrastruktur zurückgreifen können. 40-seitige Lieferscheine per Hand im Scanner zu digitalisieren – wie es bis dahin gehandhabt wurde – ist einfach nicht mehr zeitgemäß und wenig effektiv. Doch die Firma H_2O Gebäudetechnik fokussierte sich bisher vorwiegend auf das Kerngeschäft, nämlich den Handwerksbetrieb. Eine professionelle IT-Abteilung gab es im Unternehmen – bis vor kurzem – noch nicht. Man wandte sich deshalb für zukünftige Maßnahmen an faktordrei – ein IT-Fachgeschäft und Systemhaus in Detmold. Der Plan: Für den Außendienst sollten iPads angeschafft werden. Damit könnten die Mitarbeiter*innen direkt auf der Baustelle ihre Stundenzettel für die Abrechnungen führen. Zusätzlich hätten sie vor Ort Zugriff auf die relevanten Großhändlerkataloge und sie könnten mit den iPads Fotos für die Installationen und deren Dokumentation schießen. Diesmal sollte von Anfang an alles richtig geplant werden. Deshalb wurde das Detmolder Systemhaus mit ins Boot geholt.

Ein erstes Kennenlernen – mit vielen Fragezeichen.
Parallel zum Projekt rund um die iPads fiel gegenüber den Fachleuten von faktordrei noch der Hinweis, dass die hauseigene IT in den letzten Monaten „etwas komisch" geworden sei. Deshalb wurde beim Erstbesuch das digitale Equipment der H_2O Gebäudetechnik ausführlich unter die Lupe genommen. Auf den ersten Blick waren die beiden Techniker Paul Maass und Holger Coenen von faktordrei durchaus begeistert von dem, was sie in dem Handwerksunternehmen vorfanden. „Der Server war absolut auf dem neuesten Stand der Technik, ebenso wie die Bildschirme und die Rechner", erklärt Maass rückblickend. Es war also oberflächlich nichts „Komisches" in Bezug auf die IT zu finden. Trotzdem gab es die Beschwerden des Innendienstes, dass die Telefonie hin und wieder mitten im Gespräch abbrach, dass das WLAN ebenfalls nicht zuverlässig funktionierte und dass die Rechner oft sehr langsam arbeiteten.

Das Problem liegt unter der Haube.
Was auf den ersten Blick für Maass und Coenen noch unerklärlich war, ließ beim Checkup des Softwarestatus keine Fragen mehr offen. Die Entwicklung der IT-Infrastruktur verfolgte in den vergangenen Jahren kein planvolles Konzept. Das System wurde offensichtlich dem Unternehmenswachstum nur situativ angepasst und war größtenteils improvisiert erweitert worden. Somit entstanden Lücken in der Dokumentation und Schwächen im Aufbau – zum Beispiel durch den Einsatz unterschiedlicher Virenscanner, die sich gegenseitig blockierten. Die größte Schwachstelle war jedoch der nagelneue Server. Auf ihm lief noch Windows Server 2008, eine Software, für die seit Jahren keine Sicherheits-Updates mehr angeboten werden. Damit ist das Handwerksunternehmen übrigens nicht allein. Eine Recherche von Microsoft im Oktober 2021 ergab, dass in Deutschland noch 60.000 Windows Server 2008- bzw. 2008 R2-Versionen verwendet werden, was eine enorme Sicherheitslücke darstellt und zu hohen finanziellen Verlusten führen kann.

Das Worst-Case-Szenario.
Bei der H_2O Gebäudetechnik war es der Mailserver, der aufgrund der veralteten Software einem Angriff nicht standhalten konnte. Nur 2 Tage nach dem Erstbesuch wurde die Unterstützung von faktordrei erneut angefragt. Ein Trojaner hatte begonnen, die Kundschaft des Handwerksbetriebs mit infizierten Junk-Mails zu beschicken. Das führte dazu, dass H_2O-Nachrichten bei einigen Servern sofort auf die Blacklist gesetzt und die E-Mails in den Spam-Ordner verschoben wurden. „Wir konnten plötzlich keine Angebote und keine Rechnungen mehr verschicken", erinnert sich Monika Tacke, Assistentin der Geschäftsleitung in dem Haustechnikunternehmen. „Außerdem stand unser Telefon nicht mehr still. Es gab haufenweise Beschwerden."

Ein Schritt nach dem anderen.
Bevor das eigentlich geplante iPad Projekt in Angriff genommen werden konnte, musste zunächst einmal die Software auf den aktuellen Stand gebracht und – vor allem – das Mail-Server-Problem gelöst werden. Dafür konnten die Techniker von faktordrei auf ein Backup aus der Zeit vor dem Angriff zurückgreifen und wie Paul Maass es erklärt: „... das System rekonstruieren." Der Server musste zu diesem Zweck jedoch für 3 Tage offline sein, weil im Backup die aktuellen Sicherheits-Patches fehlten, die nun zunächst wieder aufgespielt wurden. Im Anschluss galt es, die Virensoftware auf allen Arbeitsplätzen zu vereinheitlichen. „Die Berücksichtigung der DSGVO wird für unsere Arbeit immer wichtiger und die Vorschriften werden immer engmaschiger", erklärt Paul Maass. Denn die Sicherheit von unternehmensinternen Daten betrifft nicht nur die Firma selbst, es sind meist auch Daten von Kund*innen, die bei einem Angriff gefährdet sind. Somit kann ein Datenverlust nicht nur kostspielig und rechtlich heikel sein, sondern auch für das Image ein echtes Problem werden.

Planungen für eine sichere Zukunft.
Die Geschäftsführung der H_2O Gebäudetechnik hatte Glück, dass sie den Kontakt zu einem professionellen IT-Unternehmen im richtigen Moment gesucht hat. „Auch Monate später erhielten unsere Kund*innen teilweise noch Spam-Mails mit unserem Absender," berichtet Monika Tacke, verärgert über den Hacker-Angriff. Die Software des Unternehmens ist nun aktualisiert, die Dokumentationen liegen vor und die Softwarelizenzen werden jetzt gesammelt verwaltet. Außerdem fährt faktordrei auf dem Server des Handwerksunternehmens eine Monitoring-Software, die zum Beispiel im Fall einer defekten Festplatte rechtzeitig Alarm schlägt. Die IT der H_2O Gebäudetechnik läuft also in geregelten Bahnen und befindet sich in sicheren Händen. Der Einführung der iPads steht nun nichts mehr im Weg.

Der nächste Schritt soll schließlich der Gang in die Cloud sein. Alle Daten sollen in Zukunft extern in der „Wolke" gehostet werden und sind infolgedessen gegen alle Eventualitäten, wie z. B. Feuer im Unternehmen, geschützt. „Wir haben aus diesen Erfahrungen gelernt", bestätigt Monika Tacke. „Mit faktordrei haben wir jetzt einen kompetenten Partner an unserer Seite. Das gibt ein sicheres Gefühl und wir können uns weiterhin auf unser Kerngeschäft konzentrieren."

Fotos © H_2O Gebäudetechnik GmbH