deviceTRUST®

KKH

deviceTRUST ermöglicht sicheres Arbeiten – auch im Homeoffice

Hybride Arbeitssituation der Versicherungsangestellten und lokalen Administratoren wird mit kontextbasierter Plattform einfacher, sicherer und transparenter

Die Kaufmännische Krankenkasse (KKH) zählt zu den führenden gesetzlichen Krankenversicherungen Deutschlands. Die Anforderung im Umgang mit den personenbezogenen Gesundheitsdaten der Versicherten sind entsprechend hoch. Um stets den optimalen Sicherheitsstandard zu gewährleisten, die Systemzugänge der lokalen Administratoren maximal zu schützen und die Telearbeit so einfach wie möglich zu gestalten, machte sich Dominik Kletke Mitarbeiter im Team IT-Infrastruktur & Architektur bei der KKH, auf die Suche nach einer passenden Softwarelösung.

Schutz vor Trojanern und unbedachtem Handeln

Bei einer großen Organisation mit etwa 4.000 Mitarbeitern, die direkt oder indirekt mit Informationen zu tun haben, die höchsten Datenschutzanforderungen standhalten müssen, steht die Datensicherheit an erster Stelle. Folglich ist man bestrebt möglichst vorausschauend zu agieren. Im Jahr 2019, einer Zeit in der Cyberattacken überproportional zugenommen hatten, entschied man sich bei der KKH deshalb für die Einführung einer zusätzlichen Sicherheitsebene. Dominik Kletke: „Wir wollten Benutzer mit erhöhten Privilegien besser absichern. Außerdem war uns klar, dass der Umgang mit USB-Sticks oder DVDs, die für den Datenaustausch genutzt wurden, kritisch werden könnte. Deshalb wollten wir ein System einführen, das diese Handhabung entsprechend absichert.“ Im Hinterkopf hatte man außerdem den Wunsch, zukünftig die Zugriffe auf diese Wechselmedien gruppenbasiert über das Active Directory steuern zu können, um auch eine weitere Absicherung der Daten zu erzielen.

Zu diesen Plänen kamen zu Beginn 2020 die Herausforderungen der Corona-Pandemie hinzu. Konkret: Innerhalb kürzester Zeit sollten so viele Versicherungsangestellte wie möglich im Homeoffice arbeiten. Das brachte eine überaus hybride System- und Arbeitssituation mit sich. Also galt es den Zugang zum Firmennetzwerk und damit auf Ressourcen der KKH, durch die Überprüfung der Aktualität und das Vorhandensein diverser Sicherheitsfeatures auf den sich einwählenden Endgeräten, abzusichern. Betroffen von dieser Situation waren ca. 3.200 Benutzer in den Servicestellen und Telearbeitsplätzen, wie man bei der KKH das Homeoffice nennt, sowie etwa 800 Büroplätze der Hauptverwaltung.

Vorsicht ist besser als Nachsicht

deviceTRUST konnte sich im Rahmen eines Vergabeverfahrens bei der KKH durchsetzen. Es bietet die beste Möglichkeit, schnell, zielführend und effektiv die Situation zu verbessern und Risiken zu minimieren. „Das ausschlaggebende Argument für deviceTRUST war, die nahtlose Integration in die bestehende Infrastruktur. Die Tatsache, dass man unmittelbar über das Active Directory gehen konnte, war für uns entscheidend, denn es eröffnete uns interessante Optionen“, erinnert sich Kletke. So kam es, dass er als Verantwortlicher für die Einführung gemeinsam mit den Kollegen, die das Active Directory und Citrix betreuen, in einer konzertierten Aktion, deviceTRUST implementierte. Zunächst wurden knapp 800 Fat Clients und über 200 Notebooks damit ausgestattet. Nach und nach erfolgte der Rollout über Citrix, so dass zum Frühsommer alle Geräte der über 4.000
Mitarbeiter über deviceTRUST abgesichert sind.

Wurden zunächst die Mitarbeiter, die trotz Pandemie in der Hauptverwaltung arbeiten mussten, versorgt, galt es im zweiten Schritt die Notebooks der Homeoffice-Mitarbeiter zu bestücken. Seither können diese über einen sicheren Datenzugang auf alle für sie relevanten Ressourcen zugreifen. Das funktioniert, indem von deviceTRUST die kontextbezogenen Informationen zusammengeführt und auf den neuesten Stand gebracht werden - sowohl lokal als auch remote. Über eine Zwei-Faktor-Authentifizierung (Hardware- und Software-Token) können die KKH-Mitarbeiter schnell, bequem und sicher auf alles, was sie für ein produktives Arbeiten benötigen, zugreifen. Kletke: „deviceTRUST hat uns geholfen, die Sicherheitsanforderungen, die das hybride Arbeiten mit sich bringt, zu erfüllen. Unsere Split-Organisation funktioniert bestens. So sind wir für die Zukunft gerüstet, denn die Telearbeit soll auch nach der Pandemie fester Bestandteil bleiben.“

> deviceTRUST sorgt dafür, dass unsere Mitarbeiter auch aus dem Homeoffice heraus sicher arbeiten können.
> Risiken, die durch Cyberangriffe entstehen, lassen sich auf diese Art und Weise erfolgreich minimieren.

Dominik Kletke, IT-Infrastruktur & Architektur
KKH Kaufmännische Krankenkasse

Mehr Sicherheit und Transparenz sowie ein besseres Trouble-Shooting

Alongside the reduction of risks and full integration, it is pleasing that user feedback on deviceTRUST has also been good. Administrators welcome the fact that they can react more quickly to any problems thanks to monitoring options and event logging. They also expect support requests to decline in the long term, as more and more errors can be prevented in advance.

In turn, users are happy not to have to worry about data security. As the system issues a warning in the event of any danger, they can actively prevent potential cyberattacks. “Employees are delighted to have a security system like deviceTRUST and the associated protection of sensitive data,” reports Kletke, detailing the positive feedback received on deviceTRUST. He is even able to envisage a scenario in which the added value and effects are so wide-reaching that old solutions can be dispensed with in the long term. “So, alongside the security improvements, we might even be able to save some money.”

> I can warmly recommend deviceTRUST to other companies – not least due to our positive experience. Anyone who operates digital workspaces should use deviceTRUST in my opinion, as it is an investment that is worthwhile and quickly pays for itself.

Dominik Kletke, IT-Infrastruktur & Architektur
KKH Kaufmännische Krankenkasse

Auf einen Blick

Herausforderung

Um den Zugriff auf USB-Massenspeicher und optische Medien abzusichern, war man 2019 auf der Suche nach einer einfachen, aber effektiven Lösung. Zunehmende Probleme mit Trojanern und die Tatsache, dass der Austausch von Daten mittels USB-Sticks und DVDs gehandhabt wurde, machte die Einführung einer übergeordneten Sicherheitsstrategie erforderlich. Auch die Absicherung privilegierter Benutzer mit Zugriff auf das Internet stand dabei im Fokus.

Lösung

Um die Situation zu lösen, wollte man auf Basis des Active Directory ein System einführen, das es erlaubt die verschiedenen Endgeräte zuverlässiger und gruppenbasiert zu schützen. Ziel war es, den digitalen Arbeitsbereich und das Homeoffice (Telearbeit) möglichst sicher, zugleich aber auch anwenderfreundlich zu gestalten. Durch die Einführung der kontextbasierten Plattform von deviceTRUST ist es der KKH gelungen, ein sicheres Arbeiten für Administratoren und Homeoffice-Anwender zu gewährleisten.

Ergebnis

Heute sind die Arbeitsplätze der Administratoren und derjenigen, die im Homeoffice arbeiten, jederzeit sicher. Über die Monitoring-Funktion von deviceTRUST kann zudem früher auf sich abzeichnende Probleme reagiert werden. Außerdem verspricht man sich, sobald deviceTRUST für alle Bereiche vollständig eigeführt ist, eine Reduktion der Support-Anfragen. Langfristig erwägt man bei der KKH zudem, vorhandene Software-Lösungen abzulösen und so die Lizenzaufwendungen zu reduzieren.

deviceTRUST®

KKH

Über deviceTRUST

Die richtige IT-Sicherheitsstrategie ist in einer hybriden Arbeitswelt unerlässlich. Mit der Kontextbasierten Sicherheits Plattform ermöglicht deviceTRUST das Arbeiten mit sicheren digitalen Arbeitsplätzen von jedem Ort, mit jedem Gerät, über jedes Netzwerk und zu jeder Zeit. Gleichzeitig gibt sie IT-Abteilungen alle Informationen und die Kontrolle, die sie benötigen, um alle Sicherheits-, Compliance- und regulatorischen Anforderungen zu erfüllen. Die starken Partnerschaften mit den führenden Technologieplattformen und die einfache Integration in jede bestehende Workspace-Management-Lösung überzeugen Kunden aus allen Branchen. Der Kontext ist immer aktuell und jede Veränderung löst eine definierbare Aktion aus. Mit dem Gerät als zusätzlichem Faktor hebt deviceTRUST die Zugangskontrolle auf die nächste Stufe und ist die optimale Ergänzung von Zero-Trust-Strategien.

Weitere Informationen finden Sie unter: **devicetrust.de**

Über KKH Käufmännische Krankenkasse

Mit über 1,6 Millionen Versicherten zählt die Kaufmännische Krankenkasse (KKH) zu den größten gesetzlichen Krankenversicherungen in Deutschland. Die KKH hat ein breites Spektrum an Versicherungsangeboten und unterstützt die Versicherten bei der Entwicklung eines gesundheitsförderlichen Lebensstils. Neben den traditionellen Versicherungsleistungen bietet die KKH u.a. ein individuelles telefonisches Gesundheitscoaching zur Unterstützung therapeutischer Maßnahmen an. In über 110 Servicestellen in allen Bundesländern beraten und betreuen rund 3.900 MitarbeiterInnen die Versicherten. Die Zentrale des Unternehmens sitzt in Hannover.

Weitere Informationen finden Sie unter: **www.kkh.de**