



„Dank der Umstellung auf die neue, tokenlose Authentifizierung werden die Zugriffe schneller erstellt und problemlos verwaltet. Die gesamte Lösung wurde vom Vorstand, der Verwaltung und dem ärztlichen Dienst gut angenommen.“

REINHARD SCHERP STELLVERTRETENDER LEITER DER EDV ABTEILUNG



KUNDE
AUF DER BULT



HERAUSFORDERUNG
Der Wechsel von einem zeitraubenden Hardware-Token-System zu einer sicheren und einfach zu handhabenden Authentifizierung



SYSTEMUNTERSTÜTZUNG
Citrix Netscaler /
Outlook Web Access



LÖSUNG
SMS PASSCODE Multi-Faktor-Authentifizierung (MFA)

Die Trägerin des grössten selbstständigen Kinder- und Jugendkrankenhauses in Deutschland sowie weiterer Einrichtungen für Kinder und Jugendliche setzt auf die SMS PASSCODE Multi-Faktor-Authentifizierung zur Sicherung ihrer Daten.

Die Hannoversche Kinderheilanstalt (HKA) nimmt in Niedersachsen bzw. Deutschland eine herausragende Stellung zur Hilfe kranker, sozial benachteiligter und behinderter Kinder ein. Im Fokus steht das Kinder- und Jugendkrankenhaus AUF DER BULT. Über 50.000 Patienten werden im Jahr versorgt.

1863 gründeten sozial engagierte hannoversche Bürger die Stiftung Hannoversche Kinderheilanstalt. Sie legten damit die rechtliche Grundlage, um die erste ärztliche Versorgungseinrichtung ausschließlich für Kinder in Hannover zu eröffnen. Heute bietet das HKA umfassende Hilfe für die Kleinen. Wie zum Beispiel das Sozialpädiatrische Zentrum (SPZ) als eines der größten und leistungsfähigsten Zentren für entwicklungsverzögerte Kinder in Deutschland. Dazu zählt auch das Cochlear Implant Zentrum (CIC) Wilhelm Hirte für taub geborene oder ertaubte Kinder sowie eine Einrichtung für heil- und sozialpädagogische Therapien für traumatisierte Kinder und Jugendliche.

Rund um das medizinische und pflegerische Angebot auf höchstem Niveau, bietet auch der administrative Rahmen Qualität und innovative Lösungsansätze. Bestes Beispiel: Die Entscheidung der IT-Verantwortlichen für die Multi-Faktor-



**AUF
DER
BULT**

HANNOVERSCHE
KINDERHEIL-
ANSTALT

Authentifizierungslösung von SMS PASSCODE. Um die Daten der Stiftung sowie der medizinischen Einrichtungen zu schützen, mussten Mitarbeiter vor ihrem Netzwerkzugriff über ein Hardware-Token ein Einmalpasscode abfragen und zusätzlich zum persönlichen Passwort eingeben.

Allerdings zählten verloren gegangene oder defekte Token, und damit Sicherheitslücken, zum Alltag der IT-Abteilung. „Neben der umständlichen Handhabung, werden selbst Kleinigkeiten wie das Wechseln der Batterien bei einer großen Anzahl zum Zeitproblem“, erklärt Reinhard Scherp, stellvertretender Leiter der EDV Abteilung AUF DER BULT. Also recherchierte das IT-Team gründlich und nahm auch die Multi-Faktor-Authentifizierungslösung von SMS PASSCODE genau unter die Lupe, und war schnell überzeugt.

Breitgefächertes Schutz

So bietet die Lösung besonders starken Schutz: Der benötigte, 6-stellige Passcode zur sicheren Identifizierung wird von der Multi-Faktor-Authentifizierungslösung SMS PASSCODE beispielsweise erst nach erfolgreicher Registrierung durch Benutzername und Passwort gesendet, und zwar in Echtzeit. Diese Methode bietet maximale Sicherheit, denn der Code ist nur für diese eine, angemeldete Sitzung nutzbar. So besteht keine Möglichkeit über das gefürchtete Phishing, also dem Versuch einer gefälschten Kommunikation, an Codes zu gelangen. Der Code ist weder vorab vorhanden, also auch nicht einsehbar, noch kann in den Generierungsprozess eingegriffen werden.

Gleichzeitig wird der Einmalpasscode in Echtzeit generiert, so dass keine vorher erstellten und bereits gehackten Passcodes zum Einsatz kommen. Die gefürchteten Brute-Force-Angriffe auf dem Passcode während des Log-In-Prozesses werden zudem erkannt und sofort gemeldet. Zusätzlich stellt die SMS PASSCODE Multi-Faktor-Authentifizierung sicher, dass der generierte Passcode auch tatsächlich beim Benutzer ankommt, egal wann und von wo aus sie sich anmelden. Dabei wird der Code zwar direkt auf dem Mobiltelefon des Nutzers angezeigt, dort jedoch nicht gespeichert. Mitarbeiter können die Codes aber ebenso per E-Mail oder Anruf erhalten, je nach Standort oder vorhandenem Endgerät.

Situationsbedingtes Sicherheitsniveau

Gleichzeitig erkennt die Software, von wo, wann oder über welches Netzwerk die Anmeldung erfolgt. Anhand dieser Kontextdaten ermittelt sie die jeweilige Bedrohungsstufe und wählt die optimale Authentifizierungsebene aus. Das persönliche Zuhause oder das Krankenhaus gelten als relativ sichere Standorte, hier ist zum Teil kein Einmalpasscode nötig. In anderen Einrichtungen oder Fremdfirmen sowie bei der Nutzung öffentlicher Funknetze erhält der Mitarbeiter ohne richtigen Einmalpasscode keinen Netzwerkzugriff.

Bei jeder Anmeldung werden also mehrere Faktoren geprüft: Standort, IP-Adresse, Art des Zugriffsystems, Anmeldezeitpunkt usw. Nach dem der Mitarbeiter seine persönlichen Zugangsdaten beim PC-Log-In auf der Eingabemaske eingegeben hat, erscheint ein weiteres Feld zur Abfrage des zusätzlichen Passcodes. Nur die korrekte Kombination aller Faktoren erlaubt den Zugriff.

„Wir haben unser Ziel erreicht. Wir verfügen über maximale Datensicherheit trotz schmalen Budget und sparen gleichzeitig Zeit, da die Handhabung, auch dank der Nutzung des persönlichen Smartphones, schnell und unkompliziert ist“, bestätigt Reinhard Scherp.



**AUF
DER
BULT**

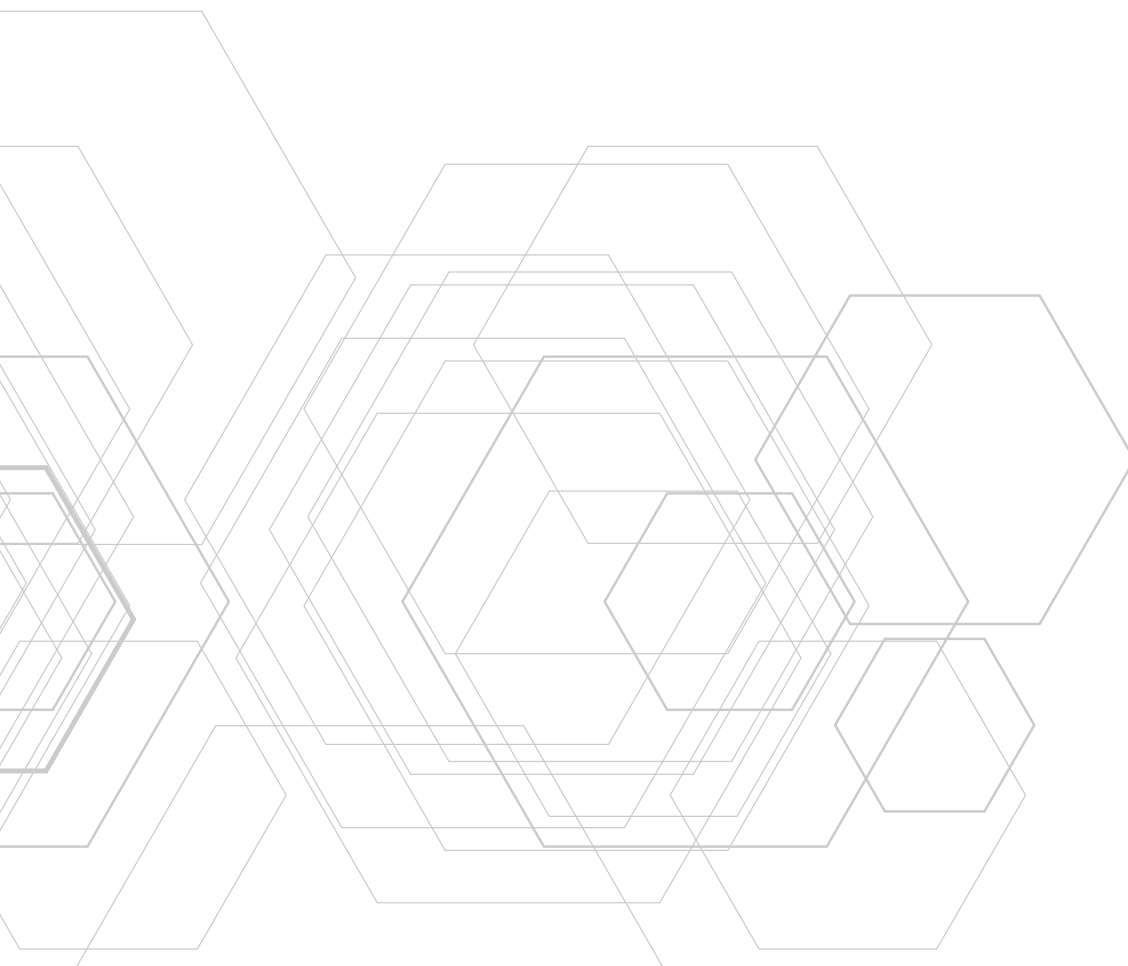
HANNOVERSCHE
KINDERHEIL-
ANSTALT

Nach einem ausführlichen Gespräch mit dem engagierten Vertrieb und dem Support der SMS PASSCODE Multi-Faktor-Authentifizierung war das neue System in nur einem Tag betriebsbereit. Vor allem externe Netzwerkzugriffe zu Citrix Netscaler und Outlook Web Access sind seit der Implementierung einfacher und schneller realisierbar. Mit aktuell 65 Zugriffslizenzen profitieren vor allem der medizinische Bereich und die Verwaltung von der neuen, sicheren Authentifizierungslösung. Weitere Lizenzen sind bereits geplant.

Fazit

Der Erfolg und die Akzeptanz bei den Mitarbeitern sprechen für sich. „Dank der Umstellung auf die neue, tokenlose Authentifizierung werden die Zugriffe schneller erstellt und problemlos verwaltet. Die gesamte Lösung wurde vom Vorstand, der Verwaltung und dem ärztlichen Dienst gut angenommen“, schließt Reinhard Scherp ab.

www.auf-der-bult.de



Entrust Datacard

1187 Park Place
Shakopee, MN 55379, USA
Phone +1 952 933 1223

Entrust Datacard Denmark A/S

Park Allé 350D
2605 Brøndby, Denmark
Phone: +45 70 22 55 33

Entrust Datacard A/S

Feringastråbe 6 Underföhring,
85774 München, Deutschland
Phone: +49 89 99216407

www.entrustdatacard.com

