Cyberresilienz – Krankenhaus-IT auf dem Prüfstand

"Wenn es um die optimale Patientenversorgung geht, ist die Verwendung von hochwertigen technischen Lösungen zur Unterstützung der medizinischen Behandlungsprozesse essenziell."

— Robin Willner, IT-Projektmanager beim Uniklinikum Dresden (UKD)

Zahlreiche Cyberattacken auf kritische Infrastrukturen – insbesondere im Gesundheitswesen – haben die IT-Verantwortlichen weltweit in Alarmbereitschaft versetzt.

Selbst Unternehmen, die sich vorbereitet wähnten, haben plötzlich Zweifel. Robin Willner, IT-Projektmanager beim Uniklinikum Dresden (UKD), zweifelt zwar nicht an der grundsätzlichen Abwehrbereitschaft des UKD. Dennoch prüft das UKD-Infrastrukturteam seine Netzwerk- bzw. Systemumgebung, um sicherzustellen, dass kein Angreifer unbemerkt Zugang erlangt hat und auf den idealen Zeitpunkt für einen Angriff wartet.

Mehr als 10.000 geprüfte Systeme.

Abdeckung von mehr als 80 Prozent der Endgeräte.

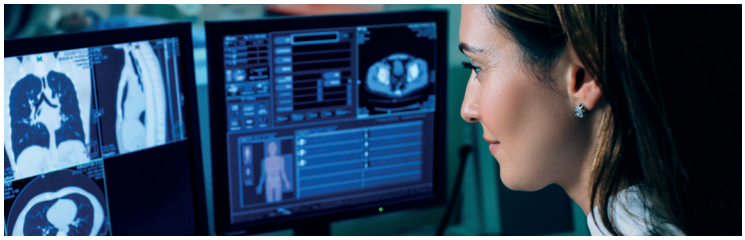
Komplettes Assessment in nur wenigen Monaten.

"In der modernen Medizin ist praktisch kein Prozess denkbar ohne IT"
Robin Willner, IT-Projektmanager beim Uniklinikum Dresden (UKD)

Exzellenz als Maßstab

Zum UKD gehören 25 Kliniken und Polikliniken, 7 Institute, 19 interdisziplinäre Zentren und rund 5.300 Beschäftigte. Als Krankenhaus der Supramaximalversorgung deckt das UKD das gesamte Spektrum der modernen Medizin ab. Für das UKD ist eine leistungsfähige IT erfolgsentscheidend: „Deshalb muss ihr Schutz höchste Priorität haben", so Willner. Dabei geht es auch um die Verantwortung des UKD als Teil der kritischen Infrastruktur und um den gesetzlichen Auftrag, Cyberrisiken vorzubeugen.

Die wichtige Rolle der IT im Gesundheitswesen



Nicht nur in der Medizin, auch in der IT gilt: Vertrauen ist die Basis des Erfolgs. Das UKD arbeitet schon seit vielen Jahren mit ISEC7 zusammen. Das Unternehmen mit Sitz in Hamburg ist BlackBerry Emerald Partner und Trusted Advisor des UKD für u. a. Mobile Business Services.

Anfang 2022 entschied das UKD, eine Analyse der Sicherheit seiner IT-Systeme durchzuführen. Das UKD und ISEC7 präferierten mit BlackBerry einen Cybersecurity-Anbieter, dessen Tools bislang noch nicht beim UKD im Einsatz waren.

Die Experten der BlackBerry Cybersecurity Services können mit ihrem Compromise Assessment (CA) detaillierte Hinweise liefern auf aktive oder frühere Cyberattacken, Datenverlust und -manipulation erkennen sowie Anomalien aufdecken, z. B. in der Nutzerauthentifizierung oder in Command & Control-Aktivitäten.

Compromise Assessment – der Weg zu mehr Transparenz

Das CA ermöglichte dem UKD eine historisch tiefgehende und global korrelierte Analyse der gesamten Infrastruktur, um frühzeitig Indikatoren für verdeckte Angriffe und unbemerkte Datenlecks zu finden und künftige Vorfälle proaktiv verhindern zu können.

Das UKD brachte BlackBerry das Vertrauen entgegen, Einblick in die erfolgskritische IT-Architektur zu nehmen und das CA ohne Auswirkungen auf den laufenden Klinikbetrieb durchführen zu können.

Zur Analyse dienten spezielle, sehr ressourcenschonende Werkzeuge von BlackBerry, welche auf die Endgeräte verteilt wurden. Dieser hohe Abdeckungsgrad war sehr vorteilhaft für die Aussagekraft des CA.

Hätte die Analyse einen verborgenen, jedoch akut laufenden Angriff aufgezeigt, so hätte BlackBerry nahtlos zu Incident Response übergehen können, um den vollständigen Ablauf der Kill-Chain und die ausgenutzten Schwachstellen nachzuzeichnen und um den Angriff zu eliminieren.

Der Abschlussbericht im Oktober 2022 zeigte glücklicherweise keine kritischen Indikatoren. Für den Vorstand wurde ein Threat Hunting Report erstellt und für die IT ein Katalog mit strategischen und taktischen Empfehlungen zur Reduzierung der Angriffsfläche, geordnet nach Risikoprioritäten.

Fazit

Rückblickend zeigen sich alle Projektbeteiligten zufrieden: „Das Krankenhaus hat einen Einblick in die Historie seiner IT-Umgebung in Bezug auf deren Sicherheitslevel gewonnen, es konnten alle Restzweifel beseitigt und ein verborgener Angriff ausgeschlossen werden."

Willner und das UKD-Team wollen das erreichte Sicherheitsniveau weiter ausbauen und eine nachhaltige Verbesserung der Sicherheit in die Praxis überführen. Kein unrealistisches Ziel, denn dank der Handlungsempfehlungen von BlackBerry konnten die internen Teams des UKD ihre eigenen Cybersecurity-Fähigkeiten weiter ausbauen. „Egal wie sicher man sich fühlt, es wird immer Optimierungspotenzial geben", weiß Willner. „Schließlich ist ein CA nur eine Momentaufnahme." Sein abschließender Rat lautet: „Ohne Budget, Ressourcen und eine gute Vorbereitung geht gar nichts."

Uniklinikum Dresden (UKD)

Branche: Gesundheitswesen

Standort: Dresden

Produkt: Compromise Assessment der BlackBerry Cybersecurity Services

Website: https://www.uniklinikum-dresden.de/de