Durch die Hinzunahme der FortiSandbox Lösung hat der Hochtaunuskreis die verbliebene Lücke zu den immer größer werdenden Risiken, insbesondere im Hinblick auf Day-Zero- und polymorphen Attacken bzw. Malware, geschlossen.

– Horst Falkenstein, Leiter IT-Service, Hochtaunuskreis

Proaktiv statt reaktiv: umfassende Sicherheit im Hochtaunuskreis dank Fortinet ATP Suite mit FortiSandbox

Der Hochtaunuskreis liegt in einem der wichtigsten Wirtschaftsregionen Europas, dem Rhein-Main-Ballungsraum. Insgesamt leben dort derzeit über 231.000 Menschen. In der Kreisverwaltung, mit Sitz in Bad Homburg, stehen der Bevölkerung rund 850 Mitarbeiter zur Unterstützung in diversen Fachbereichen zur Verfügung. Die Kreisverwaltung ist dabei in entsprechende Geschäftsbereiche wie Zentrale Dienste, Infrastruktur, Bau und Umwelt, Soziales, Arbeit, Bildung und Schule, Jugend und Freizeit strukturiert.

In Sachen Informationstechnologie ist der Hochtaunuskreis einer der modernsten Landkreise Hessens. Der IT-Fachbereich verantwortet im Landratsamt die datentechnische Versorgung der Mitarbeiter. Neben den fachspezifischen Applikationen für die diversen Bereiche verwaltet der IT-Service auch die rund 850 eMail-Konten für die Mitarbeiter. Darüber hinaus dient der IT-Service als Provider für die 59 öffentlichen Schulen, sowie für einen Teil der 13 Städte und Gemeinden im Landkreis und verschiedene kreiseigene Gesellschaften bzw. gemeinnützige Einrichtungen.

Sicherheit an erster Stelle

Angesichts der vertraulichen und persönlichen Daten und Informationen, die tagtäglich in der Kreisverwaltung verarbeitet und bearbeitet werden, genießt das Thema Sicherheit und Datenschutz im Hochtaunuskreis einen hohen Stellenwert.

Der Hochtaunuskreis setzt seit 2007 auf Fortinet Lösungen zur Absicherung des Netzes und der darin enthaltenen Systeme, Anwendungen und Daten. Mittlerweile

Sicherheit im Hochtaunuskreis

Branche: Öffentlicher Dienst

Herausforderungen

- Neuartige Malware, Day-Zero und polymorphe Attacken
- Unbekanntes, von einer klassischen Virenlösung nicht erkannter Schadcode, z.B. Ransomware in eMails (Anhänge und Links)

Ziele

- Untersuchung der in eMail enthaltenen Anhänge und Links
- Proaktiver Schutz vor unbekannten Bedrohungen

Vorteile

- Geschlossene Sicherheitslücken für einen umfassenden Schutz
- BSI-konform dank Common Criteria EAL4+ Zertifizierung

wird nahezu die komplette Infrastruktur über Fortinet-Technologien geschützt. Zu den bereits eingesetzten Lösungen zählen u.a. die leistungsstarken *FortiGate*-Next Generation Firewalls. Diese Security Gateways sichern das zentrale Netz sowie rund 60 Schulstandorte und Kreisgesellschaften am Übergang vom externen zum internen Netz u.a. mittels AntiVirus, Webfilter, IPS und Application Control ab. Auch die integrierte WLAN-Controller Funktion kommt mittels *FortiAP* Access Points zum Einsatz. Darüber hinaus sind weitere Fortinet-Lösungen der Advanced Threat Protection (ATP) Suite im Betrieb. So schützt ein *FortiWeb*-System die Web Application-Infrastruktur der Behörde, während ein *FortiMail* eMail-Sicherheitssystem die Mails zu AV und Antispam prüft sowie die (noch) zu überprüfenden Mails an die FortiSandbox weiterleitet.

So umfassend die Fortinet-Installation war, erkannte das IT-Team, dass aufgrund der zunehmenden Bedrohungen und immer raffinierterer Angriffe wie Day-Zero- und polymorphe Attacken und neuartiger Malware eine zusätzliche Absicherungsschicht nötig war. Reguläre Antiviren-Systeme können nur vor Angriffen schützen, die anhand vorab bekannter Muster eines Virus erkennbar sind. Nicht erkannt werden dagegen gänzlich neue Angriffe, die z.B. in Form von neuen, bislang noch nicht in Erscheinung getretenem Schadcode, auftreten.

Gesucht wurde daher eine Lösung, die die in eMails enthaltenen Anhänge und Links vorab untersucht und den eMail-Verkehr erst dann an den Empfänger weiterleitet, wenn die eMail als „unschädlich“ eingestuft wird. Da Fortinet genau diese Funktionalität in Form seiner FortiSandbox-Lösung im Portfolio hat, lag eine Kombination von der bestehenden FortiMail-Lösung mit FortiSandbox auf der Hand.

„Durch die Hinzunahme der FortiSandbox Lösung hat der Hochtaunuskreis die verbliebene Lücke zu den immer größer werdenden Risiken, insbesondere im Hinblick auf Day-Zero- und polymorphen Attacken bzw. Malware, geschlossen“, sagt Horst Falkenstein, Leiter IT-Service, der seit 1999 im Hochtaunuskreis tätig ist.

Leistungsstark und unkompliziert, innovativ und bewährt

Der Hochtaunuskreis schätzt die einfache und unkomplizierte Handhabung seiner Fortinet Lösungen. Das IT-Team hat viele Aufgaben und „Baustellen“. Daher werden Technologien bevorzugt, die einfach in der Installation und Bedienung sind.

Trotz der Einfachheit überzeugen die Produkte aus technischer Sicht auf ganzer Linie. So ermöglichen zum Beispiel die eigenentwickelten *FortiASIC*-Chipsätze eine hervorragende Performance. Zahlreiche ICSA- und FIPS-Zertifizierungen, NSS-Lab Empfehlungen sowie über 300 erteilte Patente unterstreichen Innovation und Qualität der Lösungen.

BSI-konform durch Common Criteria nach EAL 4+

Gerade für Behörden mit großen Mengen an persönlichen Daten spielt Vertrauen eine kritische Rolle in der Wahl des Sicherheitsanbieters. So war es für den Hochtaunuskreis von großer Bedeutung, dass Hard- und Software sowie sämtliche Services Eigenentwicklungen von Fortinet sind. Fortinet verlässt sich nicht auf Drittanbieter und legt seit der Gründung im Jahr 2000 großen Wert darauf, dass die Bereitstellung von Signaturen, Filtern und Patches aus eigener Hand kommt. Das Unternehmen hat dafür sogar eine besondere Abteilung, das *FortiGuard Advanced Threat Protection Team* mit weltweit über 250 Spezialisten. Zudem sind die FortiGate-Firewalls BSI-konform, aufgrund der Common Criteria Zertifizierung nach den strengen Vorgaben gem. Evaluation Assurance Level (EAL) 4+.

Neben der Entwicklung, Handhabung und technischer Innovation spielen die Kosten und Lizenzmodelle eine wichtige Rolle für den Hochtaunuskreis. Die im Fortinet-Preismodell enthaltene unlimitierte Benutzeranzahl sorgt für ein attraktives und einfaches Lizenzmodell, das die Behörde sofort ansprach.

Die FortiSandbox wurde in weniger als zwei Tagen vorbereitet und in Betrieb genommen. Die 1991 gegründete GORDION Data Systems Technology GmbH, ein Unternehmen für Network Security Consulting und Systemintegration, sowie Partner of Excellence von Fortinet, hat den Proof of Concept der Sandbox-Lösung aktiv begleitet und die Implementation unterstützt. Gordion begleitet den Hochtaunuskreis erfolgreich schon seit Jahren bei Themen zur Sicherheit und Netzwerken.

Seit der Installation läuft die FortiSandbox-Lösung einwandfrei. Einen reellen Risiko-Vorfall gab es laut Horst Falkenstein glücklicherweise noch nicht… „und dem soll ja auch mit dieser Lösung weitergehend vorgebeugt werden! Hier geht es auch um die Prävention möglicher Risiken“.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480