SVA REFERENZ-PROJEKT //
BEZIRKSAMT STEGLITZ-ZEHLENDORF

GANZHEITLICHE SICHERHEITS-STRATEGIE FÜR DAS BEZIRKSAMT STEGLITZ-ZEHLENDORF

Mit moderner Zero-Trust-Architektur, IGEL-Endpoints, Cisco-Netzwerk und SVA Expertise zu mehr Sicherheit und Zukunftsfähigkeit

AUF EINEN BLICK

AUFGABE

Ganzheitliche Sicherheitsmodernisierung der IT-Infrastruktur, Einführung eines Zero-Trust-Ansatzes und Stärkung der Resilienz gegenüber Cyberbedrohungen

SYSTEME UND SOFTWARE

- IGEL Workspace Edition + Enterprise Management Pack + Priority Support
- deviceTRUST für kontextbasierte Zugriffskontrolle
- YubiKey 5 NFC (1.500 Stück) + LinOTP (PoC)
- Tenable.sc + Security Center Agents
- Cisco Catalyst 9800-40 Wireless Controller + Cisco DNA Center
- Cisco Secure Firewall 3105
- VMware Horizon (Pilotierung)
- Active Directory (Härtung, Segmentierung)
- SVA CSTC Sicherheitsanalyse, Penetration-Tests & Red Teaming

BEZIRKSAMT STEGLITZ-ZEHLENDORF VON BERLIN

Das Bezirksamt Steglitz-Zehlendorf ist eine von zwölf Berliner Bezirksverwaltungen. Mit über 300.000 Bürgerinnen und Bürgern zählt es zu den bevölkerungsreichsten Bezirken der Hauptstadt. Die Verwaltung ist verantwortlich für zahlreiche zentrale Dienstleistungen – von Bürgerämtern über Bau- und Ordnungsangelegenheiten bis hin zu Jugend- und Sozialdiensten. Dabei steht der sichere und effiziente Umgang mit sensiblen Bürgerdaten im Fokus.

HERAUSFORDERUNG

Die Verwaltung in Steglitz-Zehlendorf stand vor der Aufgabe, ihre historisch gewachsene IT-Infrastruktur an die heutigen Anforderungen der Digitalisierung, IT-Sicherheit und gesetzlichen Vorgaben wie BSI IT-Grundschutz, DSGVO und KRITIS anzupassen. Besonders die Absicherung sensibler Bürgerdaten, die sichere Anbindung verteilter Arbeitsplätze und die Gewährleistung eines stabilen Betriebs waren kritisch. Veraltete Endgeräte, fehlende Transparenz über Risiken, unzureichende Zugriffssicherheit und eine Netzwerkarchitektur ohne moderne Sicherheitsmechanismen führten zu erhöhtem Administrationsaufwand und potenziellen Security-Lücken. Gleichzeitig fehlten intern Ressourcen und Know-how für eine ganzheitliche Modernisierung. Ziel war es, mit einem vertrauenswürdigen Partner eine nachhaltige Sicherheitsstrategie aufzubauen, die sowohl kurzfristige Bedrohungen adressiert als auch langfristig tragfähig ist.

LÖSUNG

SVA begleitete das Bezirksamt als *Trusted Security Advisor* von der Analyse bis zur Umsetzung einer modernen Sicherheitsarchitektur. Herzstück war die Einführung einer standardisierten Endpoint-Infrastruktur mit **IGEL Workspace Edition**, zentralem Management (EMP) und sicheren Thin Clients. Ergänzend wurde mit **deviceTRUST** eine kontextbasierte

BERLIN
Bezirksamt
Steglitz-Zehlendorf

IGEL TECHNOLOGY

CISCO
Partner

VORTEILE

- deutlich erhöhtes Sicherheitsniveau durch MFA, Netzwerksegmentierung und Schwachstellenmanagement
- spürbare Entlastung der IT-Abteilung durch zentrale Endpoint- und Netzwerkverwaltung
- Zukunftssicherheit dank modularer, skalierbarer Architektur
- Transparenz über Risiken durch Risiko-Register und Roadmap
- Stärkung der internen Kompetenz durch Schulungen und kontinuierlichen Wissenstransfer

„Die Zusammenarbeit mit SVA hat uns nicht nur eine moderne Sicherheitsarchitektur gebracht, sondern auch das Vertrauen, die digitale Transformation aktiv und sicher zu gestalten."

Mathias Altensleben & Martin Bulgrin, Bezirksamt Steglitz-Zehlendorf

Zugriffskontrolle etabliert, die nur vertrauenswürdigen Geräten Zugang zu sensiblen Verwaltungsanwendungen gewährt. Über **1.500 YubiKeys** wurden für eine starke Multi-Faktor-Authentifizierung ausgerollt – zusätzlich flankiert durch ein **LinOTP-Pilotprojekt** als flexible Open-Source-Option.

Für mehr Transparenz über Risiken führte SVA eine umfassende Sicherheitsanalyse (CSTC) durch und implementierte **Tenable.sc** für kontinuierliches Schwachstellenmanagement. Parallel modernisierte das Team die Netzwerkarchitektur mit **Cisco Catalyst 9800-40 Wireless Controllern** und **Cisco DNA Center** für Automatisierung und Segmentierung. Beratungen zur Härtung des Active Directory sowie Penetration-Tests und Red Teaming ergänzten die technische Umsetzung.

Das Projekt zeichnete sich durch enge Abstimmung mit den Fachabteilungen, gezielten Wissenstransfer und kontinuierliche Betreuung über Dienstleistungskontingente aus. Damit wurde eine Sicherheitsarchitektur geschaffen, die heutige Bedrohungen adressiert, Compliance sicherstellt und den Weg in ein Zero-Trust-Modell eröffnet.

FAZIT

Mit der Unterstützung von SVA hat das Bezirksamt Steglitz-Zehlendorf seine IT-Infrastruktur nachhaltig modernisiert und das Sicherheitsniveau signifikant erhöht. Durch die zentrale Verwaltung von Endgeräten, Netzwerken und Zugriffen konnte der Administrationsaufwand spürbar reduziert werden. Gleichzeitig sorgt die Kombination aus MFA, Schwachstellenmanagement und Netzwerksegmentierung für maximale Resilienz und Transparenz. Die Mitarbeitenden profitieren nun von stabilen, benutzerfreundlichen Arbeitsplätzen und einfacher Anmeldung per YubiKey – was die Akzeptanz und Effizienz deutlich erhöht hat.

Besonders wertvoll war die strukturierte Sicherheitsanalyse mit Risiko-Register und Roadmap, die dem Management klare Handlungssicherheit gab. Dank der modularen, skalierbaren Architektur ist die Lösung zukunftsfähig und kann bei neuen Anforderungen flexibel erweitert werden.

„Mit SVA haben wir einen Partner, der nicht nur berät, sondern uns auch bei der konkreten Umsetzung unterstützt – von der Endpoint-Modernisierung bis zur strategischen Sicherheitsanalyse. Diese enge Zusammenarbeit gibt uns Sicherheit und Vertrauen für die digitale Zukunft", bestätigen Mathias Altensleben und Martin Bulgrin vom Bezirksamt Steglitz-Zehlendorf.

KONTAKT
SVA System Vertrieb Alexander GmbH
Borsigstraße 26
65205 Wiesbaden
Tel. +49 6122 536-0
mail@sva.de
www.sva.de

BERLIN
Bezirksamt Steglitz-Zehlendorf

IGEL TECHNOLOGY

CISCO Partner