SECUREPOINT

WHITEPAPER – ANFORDERUNGEN UND LÖSUNGEN
NACH BSI-GRUNDSCHUTZ

SICHERE NETZWERKE IN KOMMUNEN

SICHERHEIT UND EFFIZIENZ

FÜR KOMMUNALE DIGITALISIERUNG

Digitale Verwaltung braucht sichere Netze

Die Digitalisierung kommunaler Dienste nimmt zu, angetrieben durch Gesetze wie das Onlinezugangsgesetz (OZG) und das E-Government-Gesetz. Dies erfordert, dass kommunale IT-Netze stärker nach außen geöffnet werden, was neue Risiken mit sich bringt. IT-Sicherheit ist daher von höchster Priorität, um Netzwerke und sensible Bürgerdaten zu schützen und gleichzeitig digitale Dienste reibungslos bereitzustellen. Der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bietet klare Leitlinien, insbesondere durch den Baustein NET.3.2 „Firewall", der Anforderungen an die Netzwerksicherheit im eGovernment-Kontext definiert.

BSI-Grundschutz NET.3.2: Zentrale Firewall-Anforderungen für Kommunen

Sicherheitsrichtlinie und Netzsegmentierung

Eine individuelle Sicherheitsrichtlinie für den Firewall-Einsatz ist Pflicht. Sie regelt, wie sensible Netzsegmente (etwa Verwaltungsnetz, Bürgerportal, Internetzugang) voneinander getrennt und vor unbefugtem Zugriff geschützt werden. Unterschiedlich vertrauenswürdige Netze müssen strikt segmentiert und Verantwortlichkeiten klar zugeordnet sein. Änderungen sind mit den Informationssicherheitsbeauftragen (ISB) abzustimmen und zu dokumentieren.

Strenges Regelwerk (Allowlist-Prinzip)

Das Firewall-Regelwerk folgt dem Allowlist-Prinzip: Nur autorisierter Datenverkehr ist erlaubt, alles andere wird blockiert. Alle Kommunikationsbeziehungen – auch zu Dienstservern in anderen Netzen – müssen explizit definiert und regelmäßig geprüft werden. Zuständigkeiten für Regelwerk-Entwurf, Umsetzung und Anpassung sind klar zu regeln.

Filter, sichere Konfiguration und Reduktion der Angriffsfläche

Das BSI fordert Stateful Inspection (also zustandsbehaftete Filter) für alle Protokolle und restriktives Filtern von technisch ausnutzbaren Elementen (z.B. ICMP oder ungültige TCP-Flags). Nur notwendige Dienste dürfen aktiv sein, überflüssige Funktionen und Schnittstellen sind zu deaktivieren. Änderungen an der Konfiguration müssen nachvollziehbar dokumentiert und durch moderne Verschlüsselung gesichert werden.

Geschützter Administrationszugang und Notfallzugriff

Admin-Zugänge zur Firewall sind streng zu beschränken – idealerweise nur von dedizierten Rechnern oder über ein eigenes Administrationsnetz. Unsichere Protokolle wie Telnet sind tabu, stattdessen sollen sichere Verfahren wie SSH und HTTPS genutzt werden. Ein örtlicher Notfallzugang muss jederzeit verfügbar sein, um im Krisenfall handlungsfähig zu bleiben.

DIGITALE SOUVERÄNITÄT UND DATENSCHUTZBESTIMMUNGEN BERÜCKSICHTIGEN

Protokollierung & Überwachung

Alle sicherheitsrelevanten Ereignisse (z.B. blockierte Verbindungen, Fehlermeldungen, Konfigurationsänderungen) müssen automatisch geloggt werden. Ein zentrales Monitoring hilft, Angriffsversuche und technische Probleme frühzeitig zu erkennen. Auch Security-Module wie IDS/IPS sind in die Protokollierung einzubeziehen.

Dokumentation und Beschaffung

Jede Änderung am Regelwerk, Wartung oder relevante Systemaktivität muss dokumentiert und vor unbefugtem Zugriff geschützt werden. Vor der Anschaffung neuer Firewalls ist eine genaue Anforderungsliste zu erstellen, die Funktionen, Zertifizierungen und Zukunftsfähigkeit (z.B. IPv6, Skalierbarkeit) berücksichtigt.

Anforderungen bei erhöhtem Schutzbedarf

Diese Anforderungen gelten als Stand der Technik und Basisschutz für alle Institutionen. Für Umgebungen mit erhöhtem Schutzbedarf sieht der IT-Grundschutz weitere Standard- und erweiterte Anforderungen vor (z. B. mehrstufige Firewall-Architekturen im „P-A-P"-Prinzip mit vorgeschaltetem Paketfilter, Application-Level-Gateway und zweitem Paketfilter, Deaktivierung ungenutzter IP-Protokolle oder temporäre Entschlüsselung des Datenverkehrs zur Bedrohungserkennung). Kommunale IT-Leiter sollten diese Maßnahmen bei besonders schützenswerten Bereichen (z. B. Polizei-, Bürgeramtsdaten, KRITIS-ähnliche Dienste oder personenbezogene Daten nach DSGVO) prüfen. Die konsequente Umsetzung der genannten Basismaßnahmen bildet ein solides Fundament, um Kommunalnetze gegen die häufigsten Angriffe zu schützen.

UTM-Firewalls: All-in-One-Schutz für Kommunen

Vielseitiger Schutz und einfache Verwaltung

UTM-Firewalls (Unified Threat Management) vereinen klassische Firewall-Funktionen mit zusätzlichen Sicherheitsmodulen wie VPN, IDS/IPS, Web- und E-Mail-Filter. Gerade im kommunalen Umfeld mit schlanker IT und begrenztem Budget bieten sie eine effiziente Komplettlösung. Sie reduzieren Komplexität, erleichtern die Administration und erfüllen viele BSI-Anforderungen „out of the box".

Praxisnutzen im eGovernment

Mit einer UTM-Firewall sichern Kommunen nicht nur den Internetzugang, sondern prüfen eingehenden Datenverkehr direkt auf Schadsoftware – und ermöglichen sicheren Remote-Zugriff via VPN. Zentrale Management-Tools helfen, Protokollierung und Dokumentation zu erfüllen. Wichtig: Die Basisanforderungen wie Segmentierung und ein sauberes Regelwerk bleiben auch bei UTM-Lösungen unerlässlich.

SECUREPOINT

IT-SICHERHEIT FÜR KOMMUNEN

Faktor Mensch und Standards zur Informationssicherheit berücksichtigen

IT-Sicherheit vervielfachen durch Awareness-Trainings

Phishing und Social Engineering sind die häufigsten Angriffsarten auf Netzwerke und gelebte IT-Sicherheitskultur die langfristig erfolgreichste Lösung zur Abwehr von Cyberattacken. Awareness Next, das Cybersicherheits-Training von Securepoint, schult Mitarbeitende darin, Risiken der digitalen Welt zu erkennen und kompetent darauf zu reagieren.

Schrittweise zum IT-Grundschutz

Cert+ ist ein herstellerneutrales Informationssicherheitsmodell, das speziell auf Kommunen und KMU zugeschnitten ist. Es bewertet die Umsetzung von Sicherheitsmaßnahmen in drei Stufen (Bronze, Silber, Gold) und orientiert sich an BSI-Grundschutz und DIN SPEC 27076. Die Bronze-Stufe deckt grundlegende Anforderungen ab, Silber und Gold führen bis an das Niveau von ISO 27001 heran.

Sicherheit und Effizienz für die kommunale Digitalisierung

Eine moderne UTM-Firewall nach Stand der Technik ist die Basis für den Schutz digitaler Verwaltungsdienste. Sie vereint effektive Abwehrmechanismen, klare Regelwerke und umfassende Protokollierung. In Kombination mit Beratungsstandards wie Cert+ und DIN SPEC 27076 gelingt der Einstieg in systematische IT-Sicherheit einfach und skalierbar. Securepoint und seine Partner bieten Kommunen dabei Technologie und Service aus einer Hand – für sichere Netze, effiziente Prozesse und digitales Vertrauen bei Bürgern.

„Made in Germany“ für die Kommunale Digitalisierung

Vertrauen durch deutsche Entwicklung

Securepoint entwickelt seine UTM-Firewalls komplett in Deutschland und garantiert „No Backdoors“ – ein Muss für digitale Souveränität in Behörden. Die Lösung kombiniert Firewall, Router und UTM in einem Gerät und unterstützt fein granulare Regelwerke, Geo-IP-Blocking und Malware-Erkennung. Ein All-Inclusive-Lizenzmodell sorgt für klare Kosten und regelmäßige Updates.

Lokale Partner für persönlichen Service

Vertrieb und Support erfolgen über zertifizierte Systemhäuser vor Ort, die auf kommunale Anforderungen spezialisiert sind. Das erleichtert Planung, Implementierung und Betrieb – und entlastet die eigene IT.

Securepoint GmbH
Bleckeder Landstraße 28
21337 Lüneburg

Tel.: +49 (0)4131 / 24010
info@securepoint.de
www.securepoint.de

SECUREPOINT

Überreicht durch Ihren Securepoint-Partner