Leistungsbeschreibung

Zentrum für Informations-, Medien- und Kommunikationstechnologie (ZIMK)

Universität Trier

54296 Trier

Öffentliche Ausschreibung für die Beschaffung einer Netzwerkinfrastruktur- und Cybersecuritylösung für das Campusnetz der Universität Trier (Next Generation Firewall mit Routing-, Management-, Sandbox- und Analysemodul sowie Honeypot)

Das Zentrum für Informations-, Medien- und Kommunikationstechnologie (ZIMK) ist der zentrale IT-Dienstleister der Universität Trier. Als Rechenzentrum der Universität betreut das ZIMK über 10.000 Studentinnen und Studenten sowie ca. 2.000 Mitarbeiter und Mitarbeiterinnen in Wissenschaft und Verwaltung auf einer zentralen IT-Infrastruktur. Die Netzwerkinfrastruktur weist eine stark segmentierte, konservative Architektur auf, mit zentralem Core-Switch als Router, mehreren Verteiler- bzw. Distribution-Switches in den Gebäuden, Außenstellen und zentralen Serverräumen, sowie jeweils ca. 300 Access-Switches und Access Points.

Kritische Datenströme werden über ein zentrales Sicherheitssystem geroutet und gefiltert, welches auch Load-Balancing von Servern leistet. Dieses System soll durch eine neue Sicherheitslösung abgelöst werden, welche die abgelösten Funktionen integriert und zusätzliche zeitgemäße Sicherheitsfunktionen für alle Netzwerkbereiche bereitstellt. Dabei steht eine Next Generation Firewall (NGFW), wiederum als hochverfügbar/redundante Hardware-Appliance, mit entsprechenden Netzwerkfunktionen im Mittelpunkt, die das zentrale Routing übernehmen soll. Zusätzlich sind weitere moderne Sicherheitsfunktionen gemäß Leistungsbeschreibung notwendig. Die zwingend erforderlichen Spezifikationen stehen nachfolgend im Text. Optionale Anforderungen sind in einem zusätzlichen Anforderungskatalog tabellarisch aufgeführt und mit Gewichtungen versehen, welche eine Bewertung entsprechender Angebote erlauben.

Zuschlagskriterien

Der Auftraggeber entscheidet über die Auftragserteilung gemäß § 58 VgV auf Grundlage des wirtschaftlichsten Angebots.

Das wirtschaftlichste Angebot ist dasjenige, das bei Berücksichtigung der folgenden Zuschlagskriterien die beste Gesamtleistung im Verhältnis zum Preis bietet:

1. **Preis**
   Der Nettogesamtpreis wird mit maximal 88 Punkten bewertet.
2. **Technische Qualität und Leistungsfähigkeit der Lösung**
   Bewertung der Erfüllung der optionalen Sollkriterien gemäß Anforderungskatalog entsprechend der jeweiligen Gewichtung bei Erfüllung des Merkmals mit maximal 192 Punkten.

Die Gesamtpunktzahl errechnet sich aus der Summe der Einzelbewertungen für Preis und Qualität. Das Angebot mit der höchsten Gesamtpunktzahl erhält den Zuschlag.

Bei Punktegleichheit entscheidet die bessere Energieeffizienz (Energie-Effizienz-Richtlinie (EU) 2023/1791 (EED)). Sollten punktgleiche und energiegleiche Angebote vorliegen, entscheidet das Los.

Preis

Der Preis wird mit maximal 88 Punkten bewertet. Das Angebot mit dem niedrigsten zulässigen Nettogesamtpreis erhält die volle Punktzahl (88 Punkte). Die Bewertung der übrigen Angebote erfolgt anhand der prozentualen Abweichung vom niedrigsten Angebotspreis. Für jedes Prozent, um das der jeweilige Angebotspreis über dem niedrigsten Angebotspreis liegt, wird ein Punkt von der Maximalpunktzahl abgezogen. Die prozentuale Abweichung wird kaufmännisch auf zwei Nachkommastellen gerundet. Negative Punktzahlen sind ausgeschlossen.

Maßgeblich für die Bewertung ist der jeweilige Nettogesamtpreis. (einzutragen in 01_Angebotsschreiben).

Technische Qualität und Leistungsfähigkeit der Lösung (Kriterien im Anforderungskatalog)

Die Bewertung der optionalen Sollkriterien erfolgt gemäß dem Anforderungskatalog unter „OPTIONALE SOLLKRITERIEN“:

- Für jedes Kriterium wird bei Erfüllung die jeweilige Gewichtung (Punkte) vergeben.
- Die Punkte werden summiert; die maximale Gesamtpunktzahl für die Qualität beträgt 192 Punkte.

Nicht erfüllte Kriterien führen zu einem Punktabzug von der Gesamtpunktzahl in Höhe der jeweiligen Gewichtung.

Die Aufteilung der Zuschlagskriterien berücksichtigt mit 88 Punkten den Preis und mit 192 Punkten die optionalen Sollkriterien (max. Gesamtpunktzahl: 280).

MINDESTANFORDERUNGEN

Technische Kurzbeschreibung

Ausgeschrieben ist eine NGFW, bestehend aus einem redundanten Verbund von zwei 19-Zoll-Geräten. Über diese Firewall soll das Routing des internen und externen Datenverkehrs der Universität Trier analog zum existierenden Core-Verbund aus Switches stattfinden, wofür entweder interne Schnittstellen oder über die Firewall verwaltete redundante Switches verwendet werden können. Die Firewall soll Zusatzfunktionen wie Logaggregation, (Compliance-) Berichterstellung und Honeypot integrieren; idealerweise vom gleichen Hersteller und auf gleicher Systemplattform. Alle Komponenten müssen mit fünfjähriger Lizenzierung und Support für Hard- und Software ausgestattet sein.

Generelle Anforderungen an alle Systemkomponenten

System und Software als Kaufmodell mit Hard- und Software-Wartungsvertrag sowie Lizenzierung über fünf Jahre

Systemkomponenten sind noch nicht abgekündigt, mindestens fünf Jahre Herstellersupport ab Abkündigung, Hardwaremodell existiert bereits zwei Jahre

Miete, auch für Lizenzen, ausgeschlossen, außer bei Systemen mit laufenden Updates (z. B. IPS)

Lieferung von originalen, neuen Produkten

Fabrikneue Komponenten von autorisierten Distributoren

Nachweis über Beschaffung erforderlich

Grauimporte nicht akzeptiert

Keine Einschränkungen von zugelassenen Netzwerkmodulen

Systeme arbeiten autonom, unabhängig von Supportstatus oder Internetverbindung

Aktuelle Firmware auf allen aktiven Systemen

IPv6-Unterstützung

Geräte sind zertifiziert

Detaillierte Produktbeschreibungen sind dem Angebot beigefügt

Datenübertragung muss höchsten Sicherheitsanforderungen genügen

Möglichst zentrales Management

Ausstattung und Lizenzierung aufeinander und auf bestehende Systeme abgestimmt

CC EAL4+ Zertifizierung für zukünftige KRITIS-Anforderungen

Auftragnehmer hat Partnerstatus beim Hersteller

deutschsprachiger Support

Verpackungen werden vom Auftragnehmer abtransportiert und entsorgt

Allgemeine Anforderung an die Firewall

HA-fähiges Firewall-Cluster

Nahtlose Übernahme der Sessions bei Ausfall

Unterstützung von aktiv/passiv und aktiv/aktiv-Betrieb

Unterstützung für mindestens drei Geräte im Cluster

Zero-Downtime Software-Upgrades

Permanente Konfigurations- und Sitzungs-Synchronisation

Failover-Aktivierung konfigurierbar

19“ Einbaumaß, max. 1HE Einbauhöhe

Zwei redundante Netzteile, hot swappable

Spezialgehärtetes Betriebssystem mit Hardware-Beschleunigung

Nicht nur Standardhardware, sondern effizienzoptimierte herstellereigene ASICs

Unbegrenzte Nutzer-/Endgerätelizenzierung

Gleichwertige Lizenzen für alle Firewall-Module

Unterstützung von IPv4 und IPv6 ohne Leistungsverlust

eigene IDS/IPS- und Applikationskontroll-Signaturen können erstellt werden

IPS-Signaturen von Drittherstellern können importiert werden

Die Firewall kann Microsoft Office und PDF-Dokumente von aktiven Inhalten bereinigen

VLAN können risikoadäquat überwacht werden

Hardwareservice, regelmäßige Schad-Signatur-Updates, Verhaltensanalysen

Anbindung ans Netzwerkmanagement mit automatisierten Benachrichtigungen

zentral verwaltbare, aber mandantenfähige Firewall-Lösung, die vollständige Trennung von Management und Firewall erlaubt, aufteilbar in virtuelle Systeme

Modulare Erweiterungen mit VMs für Analyse und Management, Sandbox, Honeypot

Spezifische Anforderung an die Firewall

Backup/Restore-Funktionalität

Die Firewall kann, bei Ausfall der zentralen Managementplattform, weiterhin vollständig via SSH über die CLI oder per Web GUI administriert werden

Multi-User-Funktionalität

Sicherung und Wiederherstellung der Konfiguration erfolgt über das Netz verschlüsselt

Unterstützung eines rollenbasierten Berechtigungskonzeptes

Unterstützung offener Programmierschnittstellen

Wenn die Appliance nicht über die Managementplattform verwaltet wird, ist die Administrierbarkeit der Appliance über eine Web-GUI ohne Applets und Plugins möglich.

Der Herstellersupport für alle Module erfolgt 24x7 (per Telefon und Mail/Web) für die gesamte Vertragslaufzeit mit einem Hardwareaustausch am nächsten Werktag.

Die zu liefernden Komponenten sind Neuware und beinhalten kompletten Herstellersupport für den deutschen Markt.

Die zu liefernden Komponenten verfügen über REST-API-Schnittstellen.

Konsolenport für Out of Band Firewall Management vorhanden

Das Firewallcluster kann ohne Unterbrechung des Netzbetriebes auf einen neuen Softwarestand aktualisiert werden

Dedizierter Ethernet Port für Firewall Management vorhanden

Die angebotene Lösung beinhaltet Material zur Verbindung der Knoten

Die Firewall beinhaltet automatische GeoIP-Listen

Die Firewall beinhaltet Content Filtering

Die Firewall beinhaltet Deep Packet Inspection

Die Firewall beinhaltet die Möglichkeit, für Mandanten mindestens 10 virtuelle Domains auf der Hardware zu betreiben.

Die Firewall beinhaltet eine automatische Schnittstelle zu allen anderen Modulen in dieser Ausschreibung

Die Firewall beinhaltet eine Unterstützung von IPSec, IKEv1 und IKEv2 Site-to-Site VPNs

Die Firewall beinhaltet eine Unterstützung von QoS

Die Firewall beinhaltet eine Unterstützung von VLANs

Die Firewall beinhaltet Firewall Regeln mit Identitity-based Access

Die Firewall beinhaltet Intrusion Detection and Prevention

Die Firewall bietet Routing, NAT und PAT

Die Firewall beinhaltet Stateful Inspection

Die Firewall beinhaltet vollen IPv4 und IPv6 Support

Die Firewall bietet eine Multi-WAN-Unterstützung und Application-based Routing

Die Firewall ermöglicht mind. 250 gleichzeitige Site-to-Site VPN-Verbindungen

Die Firewall ermöglicht Zero Trust Access

Die Firewall wird als High-Availability-Cluster mit 2 physikalischen Knoten geliefert

Durchsatz Firewalling: 200 Gbps +/- 5%

Durchsatz NGFW: 10-13 Gbps

Durchsatz IPS: 13-15 Gbps

Durchsatz SSL Inspection: 15-20 Gbps

Durchsatz Threat Protection: 9-13 Gbps

Einbauhöhe maximal 1 HE

Hardware-Appliance-basierend

Mindestens interne 12 GE RJ-45 Ports

Mindestens interne 4 QSFP28+ Ports bis 100 GbE

Die Firewalllösung integriert Routingfunktion für mindestens 32 Ports (redundant) mit 100 GbE

Redundante Stromversorgung (Hot Swappable)

Manipulationsschutz der Appliance, z. B. durch Hardware-Zertifikatsspeicher (TPM) realisiert

Zeitsynchronisierung per NTP

Zwischen den Clusterpartnern müssen sowohl Session-based, als auch Sessionless Verbindungen synchronisiert werden

Application Control-Updates automatisch durch den Hersteller

Applikationserkennung von mind. 5.000 Applikationen

Erkennung von Applikationen unabhängig von Zieladressen, Ports und Protokollen

Meldung im Browser bei HTTP(S)-basierten Applikationen

Profilbasierte Applikationskontrolle, welches variabel auf Interfaces oder Verbindungen angewendet werden kann

Alle DNS Anfragen müssen protokolliert werden

Content Filtering muss möglich sein (Wildcard + RegEx)

DNS Anfragen, welche auf Botnet C&C zurückzuführen sind, müssen geblockt werden

Es muss möglich sein, Cookies, Java Applets und ActiveX zu entfernen

Im Webfilter muss die Möglichkeit gegeben sein, einzelne Webseiten mit Ausnahmen zu versehen

Webfilter Regeln müssen per Zeitkontingent gesteuert werden können

Anzahl der vom Hersteller gelieferten IPS-Signaturen: mindestens 10000

Filterung der Pakete erfolgt in Abhängigkeit folgender Kriterien: Quell-IP-Adresse, Ziel-IP-Adresse, Netz-Adressen, Quell-, Ziel-Port und Port-Ranges

IPS Filterregeln anhand spezifischer Signaturen und Filtern

IPS-Signaturupdates automatisch durch den Hersteller

Pauschales Monitoren/Blocken von ausgehenden Botnet/C&C-Verbindunge

Profilbasiertes IPS, welches variable auf Interfaces oder Verbindungen angewendet werden kann

Ein Betrieb nach Ablauf der Lizenzen für AV Scan, IDS / IPS, Application Control muss ohne Ausfall und mit dem letzten Patternsatz ohne Umkonfiguration möglich sein.

Zentrale Lizenzübersicht

Protokollierung der Verbindungsdaten von Administrationssitzungen

Speicherung der Logdaten / Export der Daten über eine Schnittstelle

Unterstützung der Überwachung der Appliance-Funktion über SNMPv1/2c/3

Versand von Alarmen per E-Mail und/oder SNMP-Trap

Versand von Syslog-Meldungen

Der Auftragnehmer liefert den "Auftragsverarbeitungsvertrag/Data Protection Addendum" des Herstellers als Anhang mit.

Der Auftragnehmer liefert die "Technischen und organisatorischen Maßnahmen/Technical and Organizational Measures" des Herstellers als Anhang mit.

Der Hersteller der Firewalls hat das vom CISA veröffentlichte "Secure by Design"-Versprechen unterzeichnet.

Der Firewall-Hersteller besitzt eine nachgewiesene Marktetablierung, z. B. Leader im aktuellen Gartner MQ Network Firewalls und The Forrester Wave Enterprise Firewall Solutions

Der Hersteller der Firewalls ist nach ISO 9001 und ISO 27001 zertifiziert.

Die zu liefernden Firewalls sind nach Common Criteria EAL4+ zertifiziert.

Spezifische Anforderung an das Analysemodul

Implementierung als VM-Appliance

Administrierbarkeit der Appliance erfolgt über eine GUI der Appliance.

Administrierbarkeit über SSHv2 oder HTTPS (oder vergleichbar).

Das Management unterstützt folgende Authentifizierungen: Benutzername / Passwort, Zertifikate (oder vergleichbare Public-Key-Verfahren), Starke Authentisierung.

Einspielung und Aktivierung von Updates / Patches der Analyseplattform ist im laufenden Betrieb möglich, ohne dass Logdaten verloren gehen.

Multi-User-Funktionalität

Sicherung und Wiedereinspielung der Konfiguration über eine zentrale Oberfläche möglich.

Unterstützung eines Rollen-basierten Berechtigungskonzeptes

Unterstützung von Debugging-Funktionen

Unterstützung von RADIUS, TACACS+, LDAP/S

Zeitsynchronisierung per NTP

Alarmierung anhand von Logs/Filtern

Anpassung und Erstellung von eigenen Reports

Ausgabe von automatisierten Reports zeitgesteuert

Automatisierte Versendung von Reports per Mail

Das Logvolumen in GB/Tag erlaubt zumindest 30 GB.

Die angebotene Lösung bietet Multi Faktor Authentifizierung mit integrierter Tokenverwaltung.

Die angebotene Lösung ermöglicht Anbindung an externe Datenquellen / Auth Server.

Die angebotene Lösung ermöglicht die Anbindung an LDAP / Active Directory.

Die angebotene Lösung ermöglicht die Anbindung an RADIUS Server.

Die angebotene Lösung ermöglicht die Anbindung des Captive Portals an interne Systeme.

Die angebotene Lösung ermöglicht die Anbindung via SAML 2.0.

Die angebotene Lösung ermöglicht die Nutzung eines zweiten Faktors per Mobile App für 100 Benutzer.

Die angebotene Lösung ermöglicht eine zentrale Benutzerverwaltung.

Die Benutzerverwaltung ist ausgelegt für mindestens 2000 Benutzer.

Die zentrale Benutzerverwaltung wird On-premises installiert.

Einspielung und Aktivierung von Updates/Patches ist im laufenden Betrieb möglich.

Sicherung der Konfiguration über die zentrale Oberfläche möglich

Statisches Routen (IPv4, IPv6)

Unterstützte Anzahl von Geräten ist nicht durch eine Lizenz beschränkt.

Unterstützung eines hohen Kontrastmodus für Menschen mit Sehbeeinträchtigung

Unterstützung Redundanz mit Master-Slave-Modus

Unterstützung von Kollektoren für ein dezentrales Sammeln der Logs

Unterstützung von Syslog, Versand von Syslog-Meldungen

Speicherung der Logdaten/Export der Daten über eine Schnittstelle

Unterstützung der Überwachung der Appliance-Funktion bzw. System per SNMPv1/2c/3

Versand von Alarmen per E-Mail und/oder SNMP-Trap

Spezifische Anforderung an die Sandbox-Komponente

Administrierbarkeit erfolgt über eine Web-GUI ohne Applets und Plugins

Administrierbarkeit über SSHv2 oder HTTPS (oder vergleichbar)

Backup/Restore Funktionalität

Die Analyseplattform unterstützt folgende Authentifizierung: Lokaler Benutzername / Passwort; RADIUS/ LDAP

Sicherung und Wiederherstellung der Konfiguration erfolgt über das Netz verschlüsselt

Unterstützung eines rollenbasierten Berechtigungskonzeptes

Unterstützung offener Programmierschnittstellen

Anzahl lizenzinkludierter geprüfter Dateien im Monat: mindestens 20000

Customimages können über das bestehende Microsoft Licensing Agreement des Kunden lizensiert werden

Die Prüfung der Dateien erfolgt auf Basis einer aktuellen Windows 10/11 Version

Die Prüfung erfolgt mit einer aktuellen Microsoft Office Version (Office 365)

Die Sandbox erlaubt mind. 8 parallele Prüfungen

Die Sandbox hat automatische Schnittstellen zum E-Mail-Security-Gateway.

Die Sandbox hat automatische Schnittstellen zur Endpoint Protection.

Die Sandbox hat automatische Schnittstellen zur Firewall.

Die Sandbox liefert vorgefertigte Images von Windows Betriebssystemen

Zeitsynchronisierung per NTP

Protokollierung der Verbindungsdaten von Administrationssitzungen

Unterstützung der Überwachung der Appliance-Funktion über SNMPv1/2c/3

Versand von Alarmen per E-Mail und/oder SNMP-Trap

Versand von Syslog-Meldungen

Spezifische Anforderung an die Honeypot-Komponente

Administrierbarkeit erfolgt über eine GUI

Administrierbarkeit über SSHv2 oder HTTPS (oder vergleichbar)

Einspielung und Aktivierung von Updates/Patches der Analyseplattform ist im laufenden Betrieb der Firewalls möglich, ohne dass Logdaten verloren gehen

Multi-User-Funktionalität, es soll von zwei oder mehr Benutzer ein zeitgleicher Zugriff möglich sein

Sicherung der Konfiguration über die zentrale Oberfläche möglich

Unterstützung eines Rollen-basierten Berechtigungskonzeptes

Unterstützung REST-API

Unterstützung von Debugging-Funktionen

Wiedereinspielen der Konfiguration über die zentrale Oberfläche möglich

Zentrale Lizenzverwaltung in einem Portal des Herstellers

Der Honeypot kann simulieren (Decoy-OS): ESXi

Der Honeypot kann simulieren (Decoy-OS): Linux (Ubuntu, Redhat)

Der Honeypot kann simulieren (Decoy-OS): MacOS

Der Honeypot kann simulieren (Decoy-OS): Windows 7, Windows 10, Windows Server 2016, Windows Server 2019, Windows Server 2022

Der Honeypot kann simulieren (Service): Citrix

Der Honeypot kann simulieren (Service): SSH

Der Honeypot kann simulieren (Service): Tomcat

Der Honeypot kann simulieren (Service): VPN

Der Honeypot kann simulieren: IoT (Router, Switch, Printer and IP Kamera)

Der Honeypot unterstützt mind. 2 VLANs

VM-Appliance, On-premises

Zeitsynchronisierung per NTP

Speicherung der Logdaten / Export der Daten über eine Schnittstelle

Unterstützung der Überwachung der Appliance-Hardware über SNMPv1/2c/3

Unterstützung der Überwachung der Appliance-Funktion über SNMPv1/2c/3

Versand von Alarmen per E-Mail und / oder SNMP-Trap

Versand von Syslog-Meldungen

Spezifische Anforderung an das Managementmodul

VM-Appliance-basierend

Administrierbarkeit erfolgt über eine Web-GUI ohne Applets und Plugins

Administrierbarkeit über SSHv2 oder HTTPS (oder vergleichbar)

Backup/Restore Funktionalität

Die Analyseplattform unterstützt folgende Authentifizierung: Benutzernahme/Passwort, RADIUS, TACACS, SAML, LDAP

Multi-User-Funktionalität, auch gleichzeitig (User A administriert die IPS-Regeln, während User B die Firewall Policy bearbeitet)

Sicherung und Wiederherstellung der Konfiguration erfolgt über das Netz verschlüsselt

Unterstützung eines hohen Kontrastmodus für Menschen mit Sehbeeinträchtigung

Unterstützung eines rollenbasierten Berechtigungskonzeptes

Unterstützung offener Programmierschnittstellen

Zentrale Lizenzübersicht der Firewalls

Administration der Firewalls (vollumfänglich)

Erstellen von Berichten (z. B. Zugriffsberichte)

Hierarchische Objekt Datenbank

Import und Export der Konfiguration einer Firewall

Lokal gehostete Service Updates

Revisionssicherung der Konfiguration

Updates der Firewalls über die Managementplattform

Updates von Signaturen und Patterns der Firewalls über die Managementplattform zentral möglich

Workflow Prozess vorhanden (4-Augen Prinzip)

Zeitsynchronisierung per NTP

Protokollierung der Verbindungsdaten von Administrationssitzungen

Unterstützung der Überwachung der Appliance-Funktion über SNMPv1/2c/3

Versand von Alarmen per E-Mail und/oder SNMP-Trap

Versand von Syslog-Meldungen

Energieeffizienz-Anforderungen gemäß § 67 VgV (Energie-Effizienz-Richtlinie – EED)

Die zu beschaffenden technischen Geräte (Firewall-Appliance, VM-Server, Analyse- und Management-Appliance) sind energieverbrauchsrelevante Waren gemäß § 67 Abs. 1 VgV. Der Auftraggeber berücksichtigt die Vorgaben der Energie-Effizienz-Richtlinie (EU) 2023/1791 (EED) im Rahmen dieses Vergabeverfahrens.

1. **Anforderung an Energieeffizienz**
   Die angebotenen Geräte sollen das höchste bei den angebotenen Modellvarianten erreichbare Leistungsniveau an Energieeffizienz aufweisen. Soweit für die angebotenen Geräte eine Energieeffizienzklasse im Sinne der Energieverbrauchskennzeichnungsverordnung existiert, sind Geräte der höchsten Energieeffizienzklasse zu liefern.

2. **Informationen zur Energieeffizienz**
   Von den Bietern sind folgende Informationen zur Energieeffizienz zu übermitteln:

   - Angabe des Energieverbrauchs der angebotenen Geräte unter typischen Betriebsbedingungen (z. B. in Watt) sowie
   - soweit verfügbar: Erklärung zur Energieeffizienzkennzeichnung bzw. Energieeffizienzklasse des Herstellers.

Der Auftraggeber kann die übermittelten Informationen überprüfen und ergänzende Erläuterungen von den Bietern fordern.

3. **Berücksichtigung im Rahmen des wirtschaftlichsten Angebots**
   Im Rahmen der Ermittlung des wirtschaftlichsten Angebots gemäß § 58 GWB ist die Energieeffizienz der angebotenen Geräte als Zuschlagskriterium angemessen zu berücksichtigen (vgl. § 67 Abs. 5 VgV). Die Energieeffizienz wird als optionales Sollkriterium im Anforderungskatalog mit 5 Punkten bewertet.

OPTIONALE SOLLKRITERIEN

Die Erfüllung der optionalen Kriterien ist für den Auftragserhalt nicht erforderlich, wird jedoch zur Bewertung der Qualitätsunterschiede der Angebote verwendet.

erfüllt	Gewichtung bei Erfüllung	Produkt (ausblenden) Anforderung
☐	2	Alarmgenerierung bei Eventtriggern
☐	5	Alle Komponenten der Lösung können mit gemeinsamer Oberfläche interagieren
☐	3	Anbindung an ein Umbrella-Management über offene Schnittstellen
☐	2	Anpassung und Speicherung von Suchabfragen
☐	4	Anzahl lizenzinkludierter geprüfter Dateien im Monat: mindestens 30000
☐	1	Beschreibung des Lizenzmodells wird mitgeliefert
☐	4	Module enthalten automatische Schnittstellen zu anderen Modulen der Ausschreibung, zumindest Sandbox und NDR.
☐	5	Die angebotene Gesamtlösung kann mit vorhandenen Sicherheitssystemen gut verbunden werden (möglichst passende Schnittstellen, einheitliche Verwaltung)
☐	3	Das Managementmodul kann Differenzen zwischen zwei Revisionsständen anzeigen.
☐	2	Das Managementmodul kann VPN-Verbindungen verwalten.
☐	5	Der Anbieter hat eine Dependance in räumlicher Nähe und kann an Werktagen binnen einer Stunde physisch unterstützen.
☐	3	Der Anbieter kann ein Grobkonzept zur Vorstellung seiner Lösung vorlegen.
☐	5	Der Herstellen hält Nachhaltigkeitsstandards und relevante Gesetze und Vorschriften ein und berichtet regelmäßig darüber.
☐	5	Der Hersteller bietet Online-Awarenessschulungen an.
☐	5	Der Hersteller der Firewalls kann eine Marktetablierung durch Bewertung als Leader im aktuellen (2022) Gartner Magic Quadranten for Network Firewalls nachweisen.

	5	Der Hersteller der Firewalls kann eine Marktetablierung durch Bewertung als Leader im aktuellen (2024) Forrester Wave Report nachweisen.
	5	Der Hersteller führt Lifecycle Assessments nach ISO 14040/44 durch.
	5	Der Hersteller kann CO2-Emissionen im Logistik- und Transportbereich aufschlüsseln. Dabei sollten alle ab Herstellung eingesetzten Transportmittel sowie ihre CO2-Bilanz berücksichtigt werden.
	5	Der Hersteller kann darlegen, wie wirtschaftliche Nachhaltigkeit durch langfristige Unternehmensstrategien, Innovationen und Investitionen in nachhaltige Technologien sichergestellt werden.
	5	Der Hersteller kann die CO2-Emissionen nennen, die bei der Produktherstellung entstehen. Dies sollte alle Produktionsstufen und verwendeten Materialien umfassen.
	5	Der Hersteller kann die während des Betriebs und der Produktnutzung anfallenden CO2-Emissionen, einschließlich aller Lebenszyklusphasen von der Installation bis zur Entsorgung, prognostizieren.
	5	Der Hersteller kann Maßnahmen zur Verringerung von Umweltbelastungen nennen, einschließlich Energieeinsparung, Emissionsverminderung, Abfallmanagement und Wassernutzung.
	5	Der Hersteller kann Strategien und Programme zur Förderung der sozialen Verantwortung darlegen, einschließlich Arbeitsbedingungen, Weiterentwicklung der Mitarbeitenden und gesellschaftliches Engagement.
	5	Der Honeypot ist vom gleichen Anbieter wie die Firewall.
	1	Der Honeypot kann simulieren: OT-Geräte und SAP
	3	Die angebotene Lösung ermöglicht die Anbindung an weitere Systeme (z.B. SQL Server, Google, Azure/Entra ID).
	4	Die angebotene Lösung ermöglicht ein Captive Portal für mindestens 500 Gastbenutzer mit Nutzungsbedingungen bzw. Willkommensseite.
	2	Die angebotene Lösung unterstützt Novell eDirectory.
	2	Die Appliance wird auch als SaaS Variante bereitgestellt
	4	Die Benutzerverwaltung beinhaltet automatische Schnittstellen zu den anderen Modulen der

		Ausschreibung (zumindest Abgleich der Anmeldedaten mit allen Modulen).
	5	Die Benutzerverwaltung ist vom gleichen Anbieter wie die Firewall.
	2	Die Firewall enthält IoT Sicherheitsfeatures
	1	Die Sandbox hat automatische Schnittstellen zum Proxy.
	2	Die Sandbox hat automatische Schnittstellen zur Network Detection and Response.
	3	Die Sandbox hat automatische Schnittstellen zur Web Application Firewall.
	5	Die Sandbox ist vom gleichen Hersteller wie die Firewall
	3	Die Sandbox unterstützt neben Windows weitere Betriebssysteme
	2	Die Sandbox unterstützt virtuelle Maschinen zur Überprüfung auf Basis von kundenspezifischen Images.
	2	Die zentrale Benutzerverwaltung kann als SaaS bereitgestellt oder Remote installiert werden.
	5	Die zu liefernden Firewalls sind nach Common Criteria EAL4 + ALC.FLR3 zertifiziert.
	3	Es können verschiedene Windows Versionen (Windows 10 + 11) parallel zum Test verwendet werden
	2	Eventmonitoring vorhanden
	3	Integration von Management- und Analysemodul.
	2	Interner Datenträger mit mindestens 150 GB Speicherplatz
	3	MFA wird unterstützt
	3	Möglichkeit der Quarantänisierung eines Clients bei Verwendung einer blockierten Applikation / Applikationskategorie
	3	Optionale Packetprotokollierung beim Treffen einer Signatur bzw. der entsprechenden Filter-Regel
	3	Testen der Kategorien muss direkt in über die Firewall möglich sein (sowohl in der GUI, als auch auf der CLI)
	3	Unterstützung offener Programmierschnittstellen (JSON, XML)

	3	Unterstützung von verschiedenen Versionsständen der verwalteten / überwachten Systeme
	4	Wenn die Appliance nicht über die Managementplattform verwaltet wird, ist die Administrierbarkeit über SSHv2 oder HTTPS (oder vergleichbar) möglich.
	3	Zentrale Lizenzverwaltung in einem Portal des Herstellers
	4	Zero-Touch Deployment der Firewalls, inklusive Backup & Restore im Falle eines Hardwareaustausches
	3	Zwischen den Clusterpartnern müssen zwecks Redundanz zwei Heartbeat Verbindungen möglich sein.
	5	Erfüllung der Energie-Effizienz-Richtlinie – EED.
von 192 Punkten gesamt		