genua.

IT-Sicherheitslösungen für Polizeibehörden

IT-Security-Entscheider in IT-Fachbereichen der Polizei sind für ein reibungloses und sicheres Arbeiten mit einer Vielzahl von IT-Anwendungen verantwortlich. Sie müssen nicht nur die Risikozonen in den vorhandenen Infrastrukturen im Blick behalten, sondern die IT-Landschaft mit den geeigneten Technologien auch präventiv schützen. Unser White Paper zeigt Lösungswege, die diese Aufgaben vereinfachen.

SecurITy made in Germany

Inhalt.

1. Aufgabenstellungen an die IT-Sicherheit in Polizeibehörden

Erfolgreiche Polizeiarbeit ist eng mit der Funktionalität und Verlässlichkeit der eingesetzten IT-Systeme verbunden. Sowohl externe Dienste wie das Internet als auch interne Dienste wie polizeiliche Datenbanken werden täglich im Dienst genutzt. Dazu stehen Systeme der Telekommunikationsüberwachung (TKÜ) und andere interne Dienste fachbereichsübergreifend zur Verfügung. Auch die Einbindung externer Lieferanten und Dienstleister ist üblich.

Die eingesetzten IT-Systeme verarbeiten personenbezogene Daten, Ermittlungsergebnisse, Verschlusssachen und andere sensible Informationen. Es ist davon auszugehen, dass die eingesetzten IT-Systeme und die verarbeiteten Daten über einen hohen Schutzbedarf verfügen. Folglich müssen Polizeibehörden umfangreiche Maßnahmen ergreifen, um die Vertraulichkeit, die Authentizität, die Integrität und die Verfügbarkeit der eingesetzten IT-Systeme sicherzustellen.

Orientierung an BSI-Richtlinien

Eine wesentliche Hilfestellung hierbei leistet das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem IT-Grundschutzkatalog. Dieser enthält Empfehlungen, wie ein hohes Schutzniveau erreicht werden kann. Zusätzlich stellt das BSI den Behörden mit Zertifizierungen und Zulassungen einen Katalog an Produkten zur Verfügung, die unabhängig geprüft sind und nach Stand der Technik ein Höchstmaß an Sicherheit gewährleisten. Nachfolgend werden Anwendungsszenarien aus dem Polizeiumfeld dargestellt und Lösungsansätze skizziert, die sich an diesen Empfehlungen sowie an BSI-zertifizierten und -zugelassenen Lösungen orientieren.

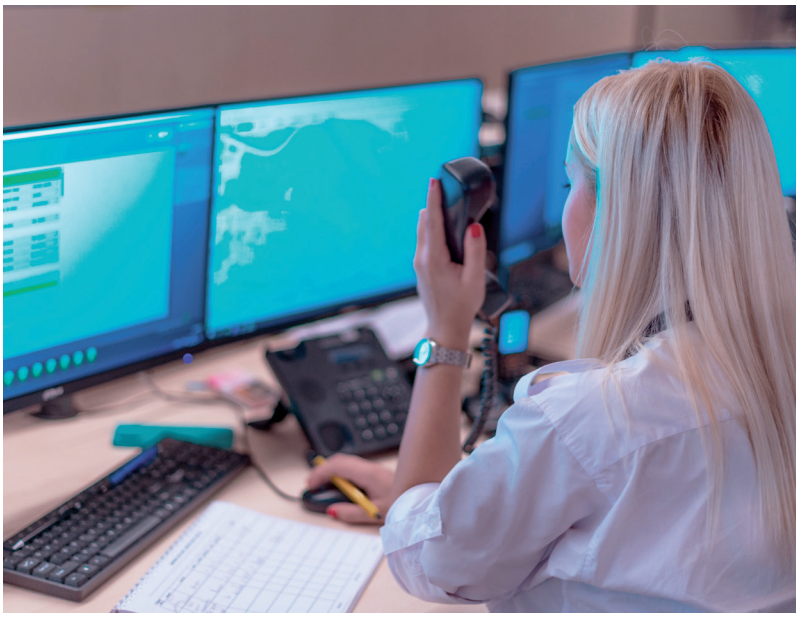
Rahmenbedingungen der IT-Sicherheit

Bei der Nutzung von externen Quellen wie dem Internet und weiteren internen Diensten werden IT-Systeme und -Netzwerke mit unterschiedlichen Schutzniveaus und Einstufungen verbunden. Die Bereiche mit unterschiedlichen Schutzniveaus sind nachfolgend als „Zonen“ bezeichnet.

Liegen unterschiedliche Schutzniveaus oder Einstufungen vor, so müssen Maßnahmen ergriffen werden, um Risiken wie z. B. Datenabfluss, Datenveränderung und Dienstausfälle zu adressieren. Im Bereich von IT-Netzwerken hat sich hierfür der Begriff der Netzübergänge etabliert. Damit ist der Überführungspunkt von zwei oder mehreren IT-Netzen mit unterschiedlichem Schutzniveau gemeint. Im Nachfolgenden wird der Begriff „Netzübergang“ für die Verbindungspunkte zwischen den unterschiedlichen Sicherheitszonen in den Netzwerken der Polizei verwendet.

> Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet Behörden wesentliche Hilfestellungen zum Schutz kritischer IT-Systeme.

2. Sichere Dienste schaffen



An der Nahtstelle zwischen Internet und lokalem Netz entscheidet sich maßgeblich das Niveau der IT-Sicherheit, da hier ein massives Sicherheitsgefälle besteht. Hier laufen die Zugriffe von außen und die von innen versandten Daten vorbei. Vorhandene Dienste wie E-Mail und Internetzugang sollen sicher angebunden und gleichzeitig weitere Dienste zur Verfügung gestellt werden, wie es bei der Telekommunikationsüberwachung oder Auskunftssystemen der Polizei der Fall ist. Viele dieser Dienste werden zukünftig mehr und mehr in die Cloud ausgelagert.

Zusätzlich existieren innerhalb der polizeilichen IT Zonen mit unterschiedlichen Sicherheitsniveaus. Dies bedeutet, dass eine unterschiedliche Kritikalität der IT-Systeme und -Netze vorliegt, z. B. beim Übergang von Management-Netzwerken zum Produktivnetzwerk oder zu Netzwerken, in die Daten aus einer TKÜ eingeleitet werden. Dies gilt natürlich auch für Netzübergänge zu anderen Behörden wie zum Corporate Network Police des Bundeskriminalamts oder zu anderen Sicherheitsbehörden. Ein besonderes Augenmerk ist hierbei auf Cloud-basierte Plattformen zu legen. Ebenfalls ist es möglich, dass bei der Anbindung anderer Dienststellen oder der Einbindung mobiler Einsatzkräfte Netzübergänge geschaffen werden.

Übergänge zwischen Sicherheitszonen schützen

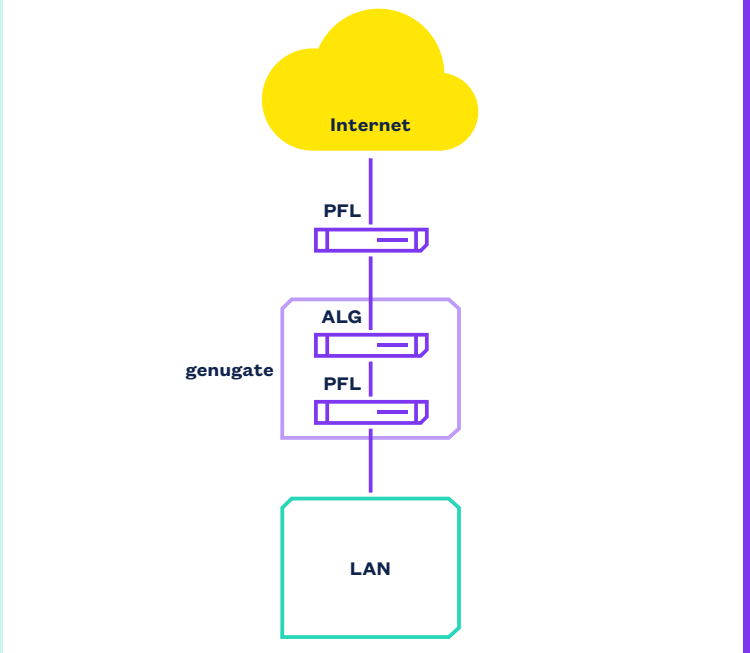
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt, beim Übergang zwischen Sicherheitszonen eine Kombination aus zwei Paketfiltern (PFL) und einem Application Level Gateway (ALG) – kurz P-A-P-Aufbau – einzusetzen: Durch die vorgelagerten Paketfilter wird das Application Level Gateway an beiden Seiten sowohl gegen direkte Angriffe als auch gegen Überlast geschützt.

Laut BSI sollten unabhängige Experten das System nach dem internationalen Standard Common Criteria (CC) in der Sicherheitsstufe EAL 4+ geprüft haben. Hierdurch haben Behörden einen unabhängigen Qualitätsnachweis und können sichergehen, dass nach aktuellem Stand der Technik das höchste Schutzniveau erzielt wird. Ein hohes Schutzniveau wird erst durch den Einsatz eines Application Level Gateways für alle Verbindungen, die über Netzübergänge verlaufen, erreicht. Denn je gründlicher die Kontrolle dieser Verbindungen erfolgt, desto stärker ist der Schutz für das gesamte Netzwerk.

Content-Analyse berücksichtigen

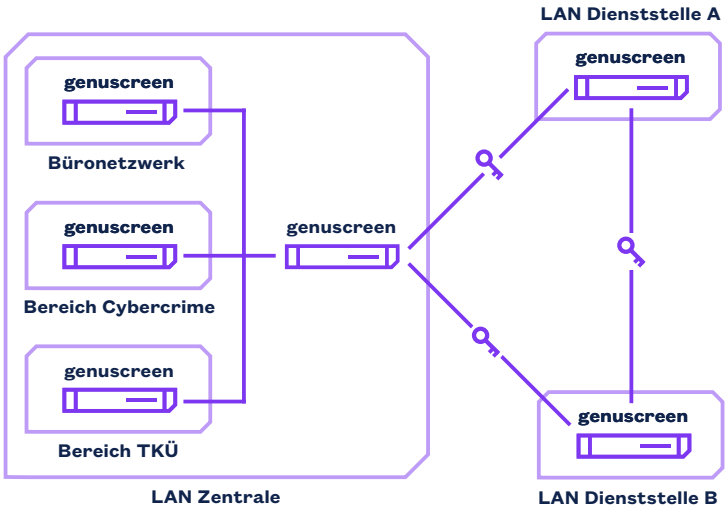
Ein zentraler Baustein ist dabei die Content-Analyse. Es werden nur Verbindungen übertragen, deren Inhalte komplett geprüft und freigegeben wurden. Nur so lässt sich gefährlicher oder unerwünschter Content sicher erkennen und blockieren. ALGs stellen Programme zur Verfügung, die das Protokoll der jeweiligen Applikation sprechen (z. B. HTTP, SMTP) und so die Daten auf Applikationsebene entgegennehmen, vollständig analysieren und auf Applikationsebene weiterreichen. Klassische ALGs sind z. B. Web Proxies oder Mail Gateways. Ein ALG kann umfangreiche Änderungen an den Daten vornehmen. So lassen sich bspw. aus Webseiten Plugins oder Skripte und aus Mails gefährliche Anhänge entfernen oder Attachements auf Viren untersuchen. Die nachfolgende Abbildung zeigt die Absicherung des Netzübergangs zwischen dem internen LAN und dem Internet mit einem P-A-P-Sicherheits-Gateway.

Schutz gemäß BSI-Empfehlung: Das zertifizierte Firewall-System genugate von genua sichert mit einem P-A-P-Aufbau die IT-Systeme von Polizeibehörden.



3. Sicherheitszonen einrichten

Im Idealfall ist die IT der Polizei in unterschiedliche Sicherheitszonen gegliedert. So sollte man z. B. das Büronetzwerk, die Fachverfahren, den Bereich Cybercrime oder die verantwortliche Stelle für die TKÜ als einzelne Sicherheitszonen realisieren. Hintergrund ist, dass nicht alle Personen bzw. IT-Systeme auf alle Dienste und Bereiche zugreifen dürfen. Bspw. sollten der Internetzugriff reglementiert oder strenge gesetzliche Vorgaben wie bei der TKÜ abgebildet werden.



Verschiedene Sicherheitszonen schaffen mit genuscreen

Natürlich sollten nur berechtigte Personen und IT-Systeme auf die internen Dienste zugreifen können. Dazu sind Maßnahmen notwendig, welche die erlaubten Kommunikationsbeziehungen zwischen den IT-Systemen wie bspw. Server, Clients, Netz- und Speicherkomponenten absichern. Hier empfiehlt das BSI, ein sogenanntes Zonenkonzept zu erstellen. In diesem werden die IT-Systeme und Dienste als logische Einheiten zusammengefasst und es wird definiert, welche Kommunikationsbeziehungen erlaubt sind.

Ein Zonenkonzept beschreibt verschiedene Sicherheitszonen mit unterschiedlichen Sicherheitseigenschaften. Das Schutzniveau der Zonen wird in zwei Schritten festgelegt. Im ersten Schritt wird der Schutzbedarf der vorgehaltenen Daten und IT-Systeme ermittelt. Im zweiten Schritt folgt die Bewertung des Risikos von IT-Sicherheitsvorfällen. Das Resultat ist der Schutzbedarf der einzelnen Zonen.

Das Zonenkonzept wird realisiert, indem man das interne Netzwerk unter Verwendung von Firewalls in separate Bereiche untergliedert. Hierbei stehen zwei unterschiedliche Typen an Firewalls zur Verfügung: entweder eine P-A-P Struktur mit Sicherheits-Gateway oder eine Paketfilter-Firewall. Sicherheits-Gateways kommen, wie im Abschnitt „Sichere Dienste schaffen“ beschrieben, bei Netzübergängen zum Einsatz. Paketfilter-Firewalls werden dazu verwendet, bei gleichem Schutzbedarf die Kommunikationsbeziehungen zwischen verschiedenen Zonen zu definieren und abzusichern. Wird ein Zonenkonzept mit entsprechenden Firewalls realisiert, können IT-Systeme und Benutzer nur die als erlaubt definierten Aktionen im internen Netz ausführen. Dies verhindert z. B. die Verbreitung von Schadsoftware über verschiedene Zonen.

Das BSI empfiehlt, dass unabhängige Experten das System nach dem internationalen Standard Common Criteria (CC) in der anspruchsvollen Sicherheitsstufe EAL 4+ geprüft haben. Somit liegt ein unabhängiger Qualitätsnachweis vor und Behörden können sichergehen, dass sie nach aktuellem Stand der Technik ein hohes Schutzniveau erzielen.

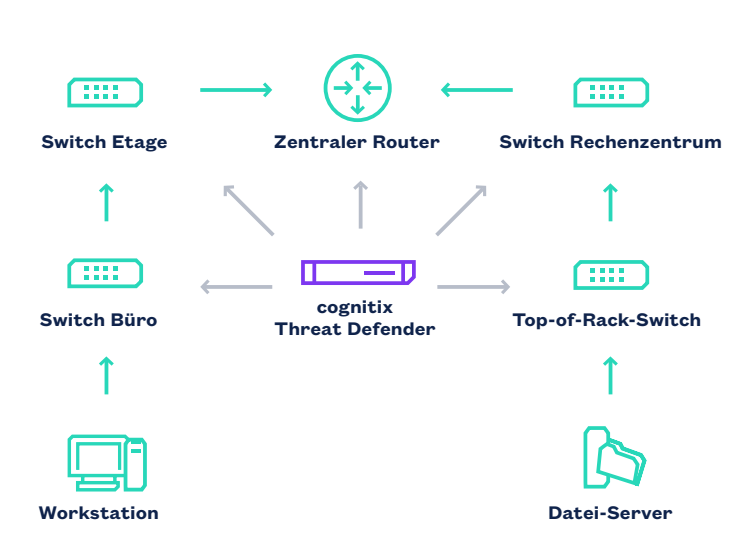
4. Vollständige Kontrolle über Netzwerkverkehr und -verhalten gewinnen

Neben Perimeterschutz und Sicherheitszonen spielt die interne Netzwerksicherheit eine zunehmende Rolle, denn die polizeilichen IT-Infrastrukturen sind z. B. durch Advanced Persistent Threats und Zero Days zunehmend auch von innen bedroht. Eine bewährte Lösung bieten Intrusion-Prevention-Systeme, die im LAN Anomalien und Angriffsmuster aufspüren und bei Gefahr automatisiert eingreifen.

Moderne IT-Sicherheitsplattformen gehen über Intrusion Prevention hinaus. Sie nutzen mit AI-, Data-Analytics- und Threat-Intelligence-Funktionen innovative Technologien, um eine zweite Verteidigungslinie im Netzwerk aufzubauen. Damit können IT-Sicherheitsbeauftragte in Polizeibehörden vorhandene Firewall-Systeme ergänzen, die den Datenverkehr an den Schnittstellen kontrollieren und sichern.

Lösungen für die interne Netzwerksicherheit erkennen alle im Netzwerk vorhandenen Geräte und verwalten diese in einer Asset-Datenbank, die mit Inventory-Systemen abgeglichen werden kann. So lassen sich Risiken durch unbekannte oder unerwartete Netzwerkteilnehmer direkt identifizieren. Eine Anomalie-Erkennung reagiert automatisch auf verändertes oder unerwünschtes Verhalten und kann auffälligen Netzwerkteilnehmern den Zugang zu bestimmten Ressourcen entziehen – ohne manuelles Eingreifen. Für umfassenden Überblick sorgt ein interaktives Echtzeit-Reporting, das den gesamten Netzwerkverkehr bis hin zu individuellen Benutzer- und Anwendungsdetails abbildet. Die in einer Lösung aufeinander abgestimmten Funktionen schaffen Transparenz und erlauben es, auf Probleme und Bedrohungen im Netzwerk gezielt zu reagieren.

cognitix Threat Defender schafft Transparenz und ergänzt als zweite Verteidigungslinie vorhandene Firewall-Systeme.



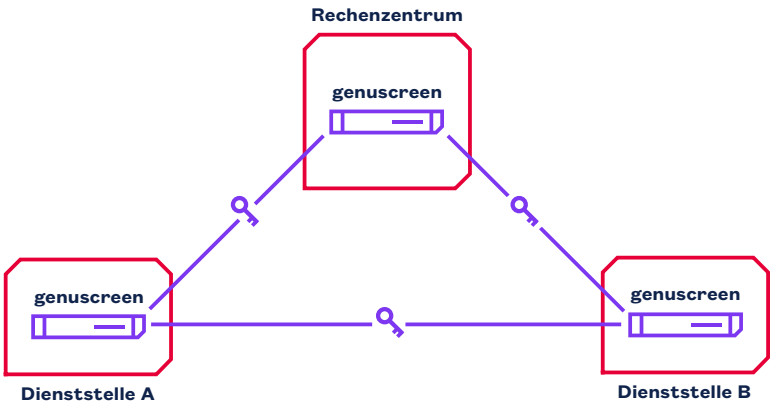
5. Standortkopplung und Anbindung weiterer Dienststellen gewährleisten

Die polizeilichen IT-Systeme und Dienste werden üblicherweise von zentralen Fachabteilungen in Rechenzentren zur Verfügung gestellt. Die unterschiedlichen Polizeibereiche sind über sogenannte Weitverkehrsnetze, etwa das Internet, miteinander verbunden. Auch die Dienststellen sind über Weitverkehrsnetze an die Rechenzentren angebunden. Weil die Weitverkehrsnetze nicht exklusiv der Polizei zur Verfügung stehen und damit die Vertraulichkeit der Daten nicht sichergestellt ist, sind Lösungen für einen sicheren Datenaustausch notwendig.

VPN-Gateways ermöglichen einen sicheren Datenaustausch über Weitverkehrsnetze und sollten zu diesem Zweck in allen Dienststellen und Rechenzentren der Polizei eingesetzt werden. Diese bauen untereinander ein sogenanntes Virtual Private Network (VPN) auf und übertragen alle Daten über verschlüsselte Verbindungen – VPN-Tunnels – durch das Weitverkehrsnetz. Somit lassen sich sensible Daten zwischen verteilten Standorten austauschen, da starke Verschlüsselungsverfahren die Vertraulichkeit garantieren.

Da es sich bei der Polizeikommunikation um höchst vertrauliche Informationen handelt, sollten IT-Security-Verantwortliche VPN-Gateways einsetzen,

die diesem hohen Schutzbedarf Rechnung tragen. VPN-Gateways mit einer BSI-Zulassung für VS-NfD erfüllen diese Anforderung. Durch ihren Einsatz ist die Übertragung VS-NfD-eingestufter Daten sichergestellt. Zusätzlich wird bei anderen sensiblen Informationen, bspw. personenbezogenen oder polizeitaktischen Daten, ein höchstmögliches Sicherheitsniveau erreicht.



genuscreen sorgt für eine hochsichere Datenübertragung in Weitverkehrsnetzen

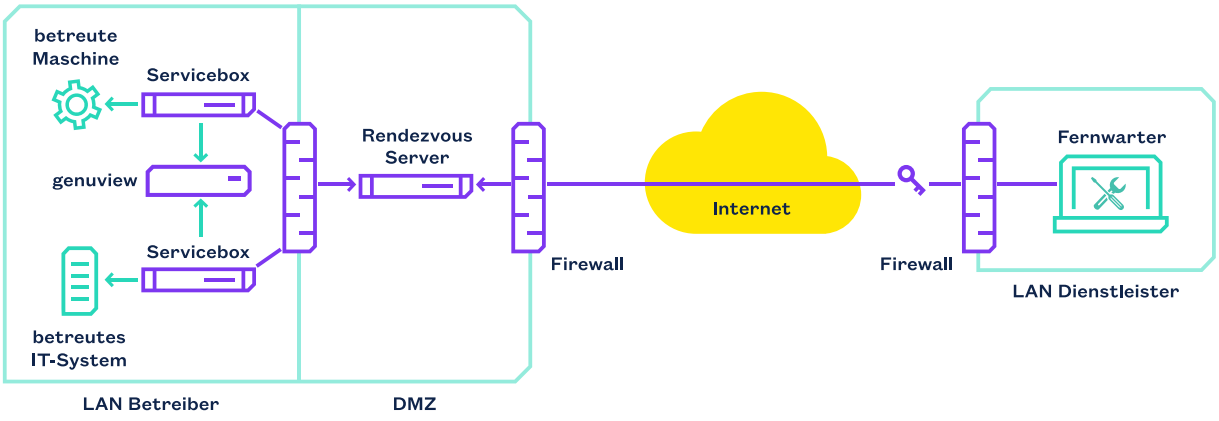
6. Sichere Fernwartung externer Dienstleister im internen Netz ermöglichen

Oftmals sind externe Spezialisten und Dienstleister für die Wartung der komplexen polizeilichen IT-Systeme zuständig. Damit Polizeibehörden diese Leistungen kostengünstig beschaffen und jederzeit flexibel Unterstützung durch die Unternehmen in Anspruch nehmen können, sollten IT-Verantwortliche einen Fernwartungszugriff einrichten. Dabei ist über physische, organisatorische und technische Maßnahmen sicherzustellen, dass ein Zugriff von außen auf die internen IT-Systeme nur durch berechtigte Unternehmen und Personen erfolgen kann.

Eine sichere Fernwartung unter Berücksichtigung der BSI-Empfehlungen ist über ein Rendezvous-System realisierbar. Dabei werden keine direkten Wartungszugriffe von externen Dienstleistern auf die Wartungsziele, z. B. ein TKÜ-System, zugelassen. Stattdessen werden alle Zugriffe des externen Personals auf einen Rendezvous Server geführt. Erst wenn ein Mitarbeiter der Polizei den Fernwartungsvorgang explizit freigibt, kann durch den externen Dienstleister ein Zugriff auf das Wartungsziel erfolgen. Dabei wird über Firewall-Regeln der Zugriff auf auf das Wartungsobjekt begrenzt.

Während des Fernwartungsvorgangs herrscht das Vier-Augen-Prinzip. Alle Aktionen, die der externe Dienstleister ausführt, können Mitarbeiter der Polizei als Bildübertragung beobachten und nachvollziehen. Dabei ist es möglich, die Fernwartungssitzung jederzeit abzubrechen. Damit sich Fernwartungssitzungen zu einem späteren Zeitpunkt kontrollieren und nachvollziehen lassen, werden alle Vorgänge umfangreich protokolliert. Zusätzlich besteht die Möglichkeit, jede Fernwartungssitzung als Video aufzuzeichnen und zu archivieren.

Sollen besonders kritische IT-Systeme durch externe Dienstleister betreut werden, wie z. B. TKÜ-Systeme, ist es erforderlich, dass die Anforderungen der Geheimhaltungsstufe VS-NfD erfüllt werden. Dazu ist die Rendezvous-Lösung mit BSI-zugelassenen VS-NfD-VPN-Gateways und VS-NfD-Client-Systemen kombinierbar. Somit lassen sich auch VS-NfD-eingestufte Systeme durch externe Dienstleister warten. Die hochsichere Fernwartungslösung ist natürlich auch für Remote Services durch interne IT-Bereiche einer Polizeibehörde nutzbar und kann so zusätzliche Kosten und Zeitaufwände vermeiden.



Die Rendezvous-Lösung erlaubt eine hochsichere Fernwartung von IT-Systemen

7. Externe Daten unidirektional in das Polizeinetz einleiten

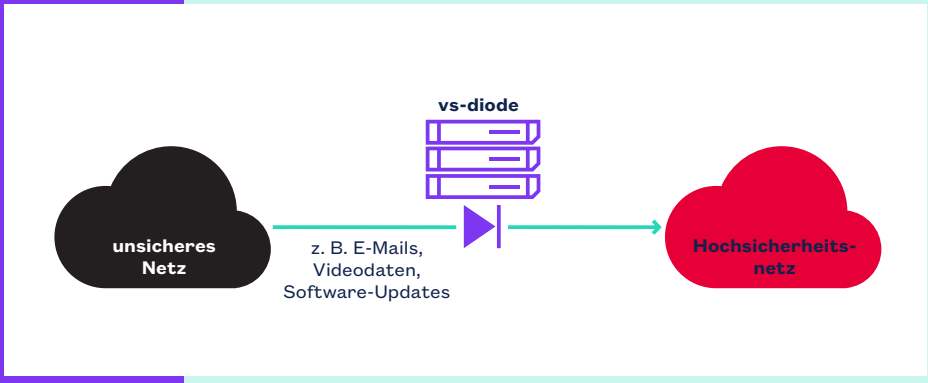
Bei Hochsicherheitszonen im Polizeinetzwerk, wie etwa Bereiche für die TKÜ, ist eine strikte Abschottung notwendig. Nur so lässt sich sicherstellen, dass keine als Verschlusssache (VS) eingestuften Informationen oder sonstige vertrauliche und sicherheitskritische Daten abfließen.

Die Hochsicherheitszone, nachfolgend rote Zone genannt, sollten IT-Security-Verantwortliche als stark isolierte Umgebung erstellen. Dafür darf auf die roten Zonen kein Zugriff aus dem Internet und keine direkte Verbindung von anderen Sicherheitszonen im internen Polizeinetzwerk möglich sein.

Damit die IT-Systeme in der roten Zone betrieben werden können, werden Daten aus niedriger eingestuften Bereichen, nachfolgend schwarze Zonen genannt, benötigt. Beispiele hierfür sind die Einleitung von TKÜ, die Übertragung von E-Mails, die Abfrage von Informationen aus Datenbanken, die Aktualisierung für Antivirensysteme oder Software-Updates. Für direkte Datentransfers in rote Zonen ohne Sicherheitseinbußen wurden sogenannte Dioden entwickelt. Diese Lösungen übertragen Nutzdaten ausschließlich in eine Richtung – von Schwarz nach Rot. In umgekehrter Richtung wird der Abfluss von Informationen per Design konsequent verhindert. So ist sichergestellt, dass an der Schnittstelle keine eingestuften Daten aus der roten in die schwarze Zone gelangen können.

Zusätzlich zum Einbahn-Datentransfer sollte eine Diode den Betrieb eines strikt auf Statusmeldungen begrenzten Feedback-Kanals in Gegenrichtung ermöglichen, da Protokolle wie FTP, SMTP und TCP diese Statusmeldungen benötigen, um die schnelle und zuverlässige Datenübertragung zu gewährleisten. Über eine BSI-Zulassung ist sichergestellt, dass die Lösung dem aktuellen Stand der Technik entspricht und die gesetzlichen Vorgaben erfüllt.

vs-diode ermöglicht die unidirektionale Kommunikation in Polizeinetzen.



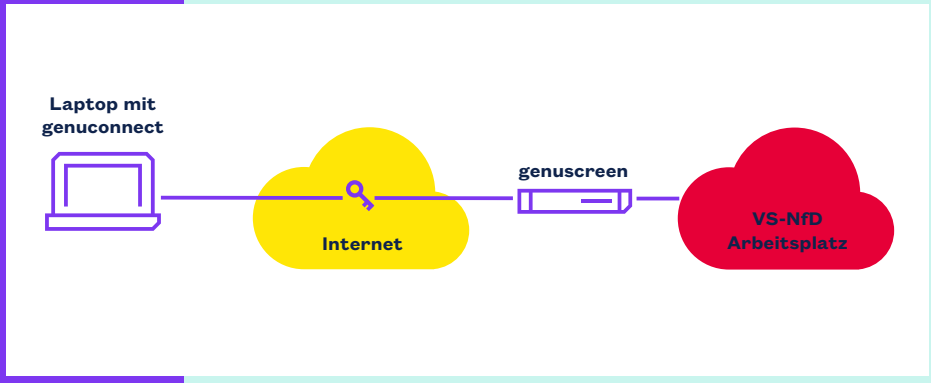
8. Mitarbeiter im Home Office, mobile Einsatzkräfte und kleinere Dienststellen sicher anbinden

Die internen Polizeisysteme, wie z. B. Vorgangsbearbeitungssysteme oder Aufklärungsdatenbanken, stellen wertvolle Informationen bei operativen Polizeimaßnahmen zur Verfügung, etwa bei Personenkontrollen oder Großveranstaltungen. Damit mobile Einsatzkräfte, Einsatzfahrzeuge oder auch Administratoren von außen auf die internen Daten und Systeme zugreifen können, ist eine Möglichkeit zum Remote-Zugriff notwendig.

Ein sicherer Fernzugriff wird mit sogenannten VPN-Lösungen über einen Internetanschluss, z. B. DSL oder LTE, realisiert. Dazu wird ein VPN-Gateway im Rechenzentrum eingesetzt und die mobilen Einsatzkräfte, Administratoren und Heimarbeitsplätze erhalten einen VPN Software Client auf einem Standard-PC. Diese Lösung baut dann ein Virtual Private Network zum Rechenzentrum auf und überträgt alle Daten mit verschlüsselten Verbindungen – VPN-Tunnels – über den Internetanschluss. So sind sensible Informationen von Personen oder Systemen außerhalb der Polizeiinfrastruktur nutzbar, weil starke Verschlüsselungsverfahren die Vertraulichkeit garantieren.

Da bei der Polizeikommunikation höchst vertrauliche Daten ausgetauscht werden, sollten Polizeibehörden nur VPN-Gateways und Endgeräte einsetzen, die diesem hohen Schutzbedarf Rechnung tragen. VPN-Lösungen mit einer BSI-Zulassung für VS-NfD erfüllen diese Anforderung. Ein Einsatz BSI-zugelassener Produkte stellt sicher, dass VS-NfD-eingestufte Daten übertragen werden dürfen. Zusätzlich wird bei anderen sensiblen Informationen, bspw. personenbezogenen oder polizeitaktischen Daten, ein höchstmögliches Sicherheitsniveau erreicht.

Mit genuconnect können mobile Einsatzkräfte hochsicher auf vertrauliche Informationen zugreifen.



Weitere Informationen:

www.genua.de/it-sicherheitsloesungen

Mit Lösungen der genua GmbH können Sie auch Cloud-Infrastrukturen, Telefonie und Digitalfunk absichern. Wir unterstützen Sie bei der technischen Planung, der Beschaffung, der Inbetriebnahme und dem Betrieb von IT-Sicherheitslösungen im Polizeibereich.

Kontaktieren Sie uns: vertrieb@genua.de oder +49 89 991950-902

WP-PLZ-1023-04-DE

Über genua

Die genua GmbH ist Enabler der digitalen Transformation. Wir sichern sensitive IT-Netzwerke im Public- und im Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimschutzbetreuten Industrie mit hochsicheren und skalierbaren Cyber-Security-Lösungen. Dabei fokussiert sich die genua GmbH auf den umfassenden Schutz von Netzwerken und Kommunikation sowie auf die interne Netzwerksicherheit für IT und OT. Das Lösungsspektrum reicht von Firewalls & Gateways, VPNs, Fernwartungssystemen, interner Netzwerksicherheit und Cloud Security bis hin zu Remote-Access-Lösungen für mobile Mitarbeiter und Home Offices.

Die genua GmbH ist eine Tochtergesellschaft der Bundesdruckerei-Gruppe. Mit mehr als 400 Mitarbeitenden entwickelt und produziert sie IT-Security-Lösungen ausschließlich in Deutschland. Seit der Unternehmensgründung 1992 belegen regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den hohen Sicherheits- und Qualitätsanspruch der Produkte. Zu den Kunden zählen u. a. Arvato Systems, BMW, die Bundeswehr, das THW sowie die Würth-Gruppe.

genua GmbH
Domagkstraße 7 | 85551 Kirchheim bei München
+49 89 991950-0 | info@genua.de | www.genua.de