secunet

Sichere Fernwartung von Anlagen

Ganzheitliche Lösungen für Servicetechniker

Im Zuge des Digitalisierungstrends wird heute nahezu alles vernetzt und zunehmend auch aus der Ferne gewartet – weltweit. Dadurch steigt die Gefahr vor Diebstahl produktions- und versorgungsrelevanter Informationen sowie Manipulation und Sabotage.

Neben hohen Sicherheitsmaßnahmen, die vor Ort an den Leitstellen und Anlagen zu treffen sind, müssen auch die Arbeitsplätze zur Fernwartung alle Sicherheitsanforderungen nach aktuellem Stand der Technik erfüllen. Ganzheitlich sichere End-to-End-Konzepte sind folglich gefragt.

Für Servicetechniker sind Fernzugriffsmöglichkeiten über das Internet ein Segen, da vieles zentral vom Standort des Lieferanten aus als Service bereitgestellt werden kann. Infolge sind zahlreiche Reisen nicht mehr erforderlich. Die Einbindung der Spezialisten wird schneller und kosteneffizienter realisiert. Ausfälle werden bei rechtzeitigem beziehungsweise proaktivem Eingriff vermieden und schneller beseitigt. Die Wartungskosten reduzieren sich und die Verfügbarkeit steigt.

Der privilegierte Fernzugriff zur Wartung von Leitstellensystemen und Anlagen schafft Mehrwerte:

- Sicherheitspatches und Funktionsupgrades einspielen
- Funktionen freischalten / deaktivieren
- Bedienerunterstützung
- Fehlerauslesung, -diagnose und -behebung
- Auslesen von Betriebs- bzw. Zustandsdaten der Anlagen
- Unterstützung von Wartungsarbeiten
- Predictive Maintenance
- Optimierung des betrieblichen Energiemanagements
- Anwenderkonten aktivieren / deaktivieren

Eingriff am offenen Herzen

Doch man muss sich vor Augen führen, dass die Internet-basierte Fernwartung von SCADA-Systemen und Stationssteuerungen der Versorgungswirtschaft sowie von Maschinen und Anlagen der Industrie vielfach einer Operation am offenen Herzen gleicht. Deshalb müssen viele Sicherheitsmaßnahmen in der Prozess-IT (OT) getroffen werden, um potenzielle Angriffsvektoren aus dem Internet oder aus dem Office-Netz zu minimieren. Gängige Praxis sind beispielsweise Whitelisting, Netzwerksegmentierungen und dedizierte Portfreigaben, Logging, um einen für die Gesamtanlage möglichst sicheren und in der Prozess-IT auch steuerbaren, VPN-basierten Fernzugriff zu schaffen. Diese und zahlreiche weitere Sicherheitsmaßnahmen müssen Betreiber in Zusammenarbeit mit den Herstellern bzw. Integratoren umsetzen. Doch steht das Thema IT- und OT-Sicherheit nach Stand der Technik bei Anlagenherstellern, Integratoren und Betreibern nicht immer im Fokus.

Hinzu kommt auch die Herausforderung, dass nicht nur der Schutz der kritischen Systeme beim Betreiber vor Ort entscheidend ist: Wer Manipulation oder Spionage betreiben und dafür u.a. Malware einbringen will, findet über den Rechner des Servicetechnikers eines der bequemsten und zunehmend genutzten Einfallstore. Deshalb sind besonders an die Notebooks und Workstations der Servicetechniker höchste Sicherheitsanforderungen zu stellen. Selbst bei Diebstahl des Servicesystems muss die Sicherheit der Leitstellen und Anlagen gewährleistet bleiben.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt deshalb ganzheitlich sichere Zugangsdienste. Sie kommen idealerweise aus einer Hand und umfassen neben der Bereitstellung einer End-to-End sicheren Einwahl zur Leitstelle oder Anlage vor Ort auch den vollumfänglich sicheren Remote Access-Arbeitsplatzrechner für den Mitarbeiter.

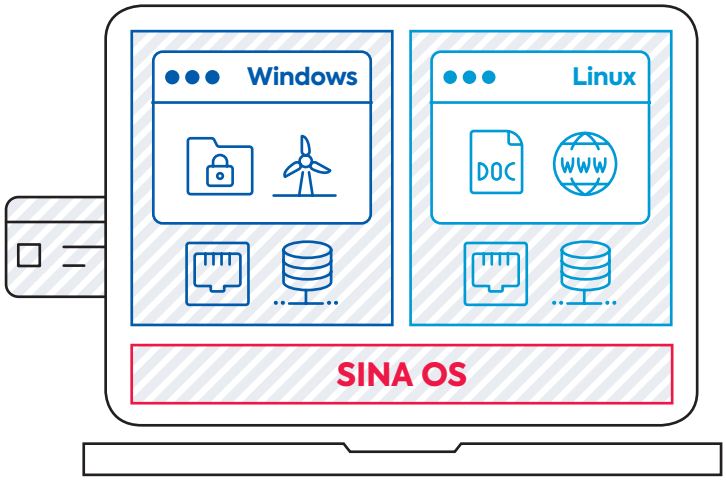
Ganzheitliche Fernwartungslösungen

Genau für solche Anwendungen ist die vom BSI zertifizierte Sichere Inter-Netzwerk Architektur (SINA) von secunet ausgelegt. Ursprünglich für den sicheren Informationsaustausch in Bundesbehörden konzipiert, kommt sie nun auch in zahlreichen KRITIS-Infrastrukturen sowie bei weiteren, zunehmend sicherheitssensitiven industriellen Anwendungen zum Einsatz. Dies liegt darin begründet, dass die zunehmende Digitalisierung leider gleichzeitig auch neue Angriffsflächen schafft. Auch deshalb hat u.a. der Gesetzgeber neue Gesetze zum Schutz der Kritischen Infrastrukturen (KRITIS) geschaffen. Der Ausfall oder Beeinträchtigung der kritischen Dienstleistungen können schließlich zu nachhaltig wirkenden Versorgungsengpässen, erhebliche Störungen der öffentlichen Sicherheit oder zu anderen dramatischen Folgen führen. Fernwartungslösungen für Leitstellen und Anlagen sollten deshalb bestmöglich geschützt werden.

„Komfortables Arbeiten und bestmöglicher Schutz sind keine Gegensätze.“

Bauen Unternehmen beim Remote Access auf SINA-Workstations und die ganzheitliche Infrastruktur des SINA-Ökosystems, entscheiden sie sich für den – nach dem Stand der Technik – bestmöglichen Schutz, ohne bestehende und neue Anwendungsbereiche einzuschränken.

Die SINA Workstation liefert alle Kernfunktionen, die man für sichere Remote Access-Clients als Basistechnologie benötigt, als aufeinander abgestimmte All-in-One Lösung. Hierzu gehört die Hardware als solche, das gehärtete SINA Betriebssystem mit hochwertiger Festplattenverschlüsselung, verschlüsselte Netzwerkverbindungen, eine Benutzerverwaltung in Echtzeit, Zwei-Faktor-Authentisierung, sowie einer Policy-basierten Schnittstellenkontrolle. Installiert werden muss lediglich die eigentliche Anwendersoftware in der speziell für den Anwendungsfall passgenau konfigurierten Virtuellen Maschine (VM).



Auf einer SINA Workstation lassen sich mehrere virtualisierte Arbeitsplätze für die Fernwartung parallel nutzen

Sicher ist sicher

Die innerhalb der SINA Workstation genutzten virtualisierten Gastsysteme mit ihren spezifischen Anwendersoftwareinstallationen (Arbeitsplätze für unterschiedliche Aufgaben und Sicherheitslevel) können ausschließlich die Schnittstellen verwenden, die die im zentralen SINA Management definierten Policies erlauben. Auch innerhalb der Kommunikationsschnittstelle wird der Datenverkehr kontrolliert, da auf allen Kommunikationsendpunkten Policy-basierte Firewall-Systeme implementiert werden, deren Regelwerk nur im zentralen Managementsystem administriert werden kann.

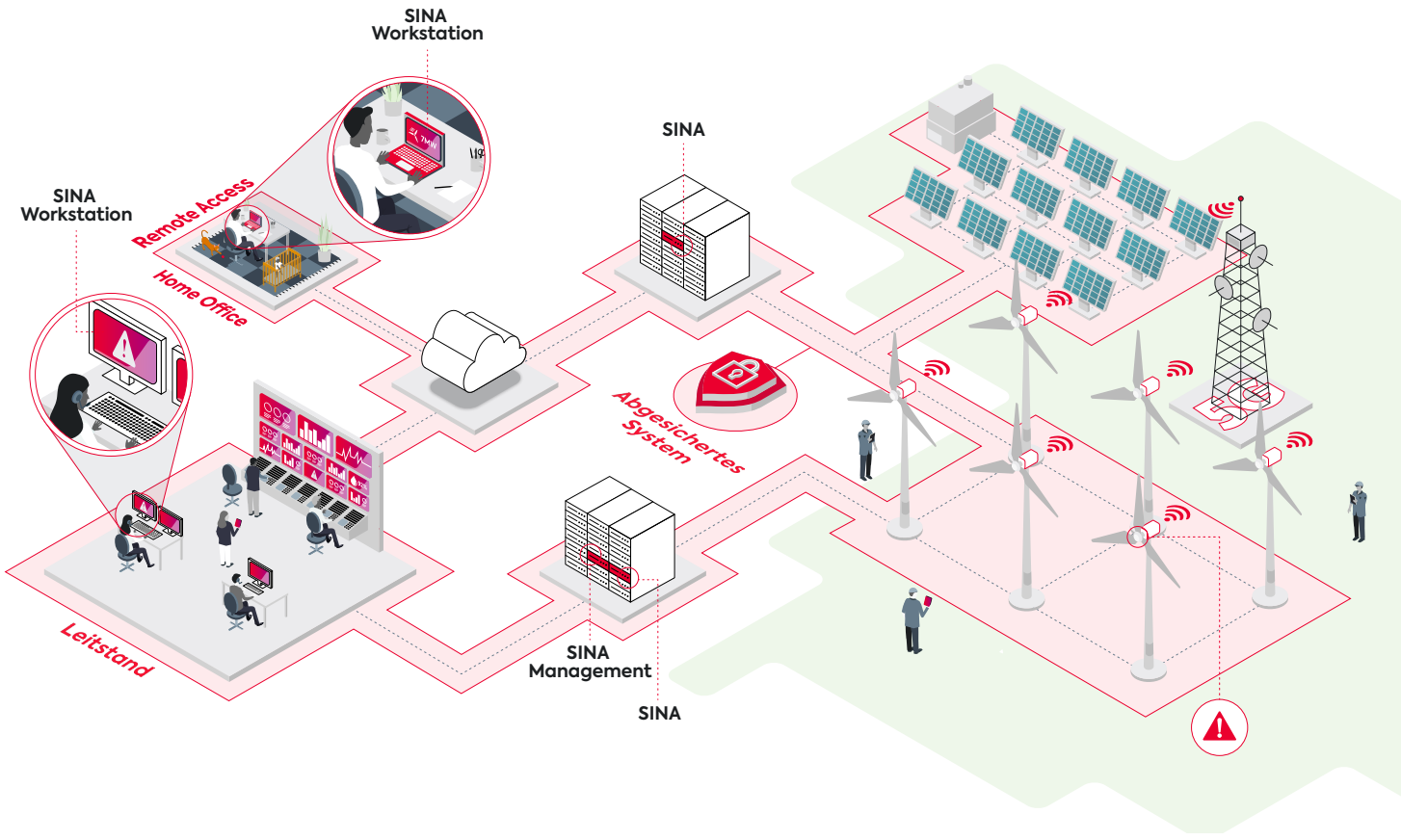
Einfache Integration, flexible Skalierbarkeit

SINA-Lösungen für den Remote Access bestehen in der Minimalkonfiguration aus einer SINA-Workstation und einer SINA-Box, die beim Betreiber als Gateway zur Leitstelle oder Anlage installiert wird. Beide Komponenten sind ausschließlich als Hard- und Software-Bundle erhältlich, um höchste Qualitäts- und Sicherheitsansprüche nach dem Stand der Technik sicher zu stellen. Das für den Betrieb notwendige Managementsystem für die SINA-Installation kann dabei sowohl bei secunet als auch bei dem einzusetzenden Unternehmen selbst oder einem Dritten betrieben werden.

Mit dem SINA-Ökosystem können selbst komplexeste End-to-End sichere Netzwerke orchestriert werden – Fernwartungs-Installationen mit mehr als 20.000 installierten SINA-Workstations und sehr individuellen Berechtigungsvergaben sind möglich.

Kunden sind sowohl KRITIS-Unternehmen, die mit ihren Lösungen den Fernzugriff auf ihre Leitstellen und verteilten Anlagen ermöglichen als auch Industrieunternehmen, die ihre IT und OT auf höchstem Sicherheitsniveau absichern.

Visualisierung des vereinfachten Netzaufbaus



Ein Remote Access für Maschinen und Anlagen besteht aus einer SINA-Workstation, einem sicheren SINA-Endpunkt zu den Maschinen und Anlagen beziehungsweise Netzwerksegmenten und dem SINA-Managementsystem.

Nachhaltige, vom BSI geprüfte Sicherheit

Der Stand der Technik für IT-Sicherheit ist auch in Zukunft für das SINA-Ökosystem gewährleistet: Alle Änderungen, Weiterentwicklungen und Funktionserweiterungen an SINA-Produkten geschehen in enger Abstimmung mit dem BSI. Eine Investition in SINA bietet damit einen nachhaltigen Schutz für die Digitalisierung. Speziell der Stand der Technik im Rahmen der IT-Sicherheit ist in KRITIS-Infrastrukturen gesetzlich notwendig.

SINA bietet mit der vom BSI geprüften Sicherheit alle Voraussetzungen für einen wirksam gesicherten Remote Access.

Wer hohe Sicherheit sucht, findet keine Alternative

Sie sind unsicher, ob es noch alternative Lösungen gibt, die ebenfalls ihren Zweck erfüllen? Was das Remote Access-Arbeiten betrifft, gibt es diese sicherlich. Die Vorteile bei SINA im Überblick:

- BSI geprüftes Gesamtsystem inkl. ganzheitlicher Sicherheitsarchitektur
- Kontinuierliche Weiterentwicklung unter Berücksichtigung aktueller Bedrohungslagen
- Beratung und Integrationssupport durch den Hersteller und geschulte Betreiber bzw. Partner
- Sichere Benutzer-Administration mit aktiver Sperrmöglichkeit inkl. Schnittstellenkontrolle
- Einsatz von sicheren Boot-Prozessen
- Sicherung des privaten Schlüssels vor unberechtigtem Kopieren auf einer sicheren Smartcard (Zwei-Faktor-Authentisierung)
- Zentrales Management- und Monitoringsystem für verteilte Installationen
- Möglichkeit verschiedenster voneinander getrennter Einsatzszenarien auf einem Gerät (z.B. Zugriff auf Office-IT über Session 1 und Zugriff auf die Prozess-IT über Session 2)
- Robuste Reaktionsmöglichkeiten zum Weiterbetrieb bei kompromittierten Gästen
- Einsatz von sicheren Backup-Systemen zur Sicherung vor Verlust von Daten

Fordern Sie noch heute ein SINA-Sicherheitskonzept für den Remote Access auf Ihrem Leitstand oder Ihrer Warte an.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com

secunet – Schutz für digitale Infrastrukturen

secunet ist Deutschlands führendes Cybersecurity-Unternehmen. In einer zunehmend vernetzten Welt sorgt das Unternehmen mit der Kombination aus Produkten und Beratung für widerstandsfähige, digitale Infrastrukturen und den höchstmöglichen Schutz für Daten, Anwendungen und digitale Identitäten. secunet ist dabei spezialisiert auf Bereiche, in denen es besondere Anforderungen an die Sicherheit gibt – wie z. B. Cloud, IIoT, eGovernment und eHealth. Mit den Sicherheitslösungen von secunet können Unternehmen höchste Sicherheitsstandards in Digitalisierungsprojekten einhalten und damit ihre digitale Transformation vorantreiben.

Über 1000 Expert*innen stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft. Zu den Kunden zählen die Bundesministerien, mehr als 20 DAX-Konzerne sowie weitere nationale und internationale Organisationen.
Das Unternehmen wurde 1997 gegründet. Es ist an der Deutschen Börse gelistet und erzielte 2024 einen Umsatz von rund 407 Mio. Euro.

secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen
T +49 201 5454-0 · info@secunet.com
secunet.com

secunet