Ein ganzheitliches, NIS2 konformes Sicherheitskonzept für Kritische Infrastrukturen in Deutschland

Ab 18. Oktober herrscht in Deutschland Anwendungspflicht: NIS2 erhöht die EU-weit geltenden Sicherheitsbestimmungen für KRITIS-Betreiber. Sie stuft zirka doppelt so viele Sektoren als kritisch ein, stockt Bußgeld empfindlich auf und führt neue Pflichten in der IT-Sicherheit ein – für deren Verletzung die Geschäftsleitung haftet. Die geforderte Resilienz erreicht eine Umwandlung gewachsener, aus einer Fülle von Komponenten zusammengesetzter Legacy-Systeme in eine ganzheitliche IT-Infrastruktur.

Eine ganzheitliche IT-Infrastruktur muss einen Schutzschirm gegenüber unerwünschten Einflüssen von außen und innen aufbauen und die Verfügbarkeit und Skalierbarkeit sicherstellen.

Betreiber Kritischer Infrastrukturen (KRITIS) sehen sich in der aktuellen geopolitischen Lage unterschiedlichen Bedrohungsszenarien ausgesetzt. Gleichzeitig sind sie mit komplexen regulatorischen Rahmenbedingungen konfrontiert. Auf nationaler Ebene spielt insbesondere das BSIG − welches bereits mehrfach durch IT-Sicherheitsgesetze aktualisiert und von der BSI-Kritisverordnung konkretisiert wurde − eine zentrale Rolle. Dieses wird durch Spezialgesetze z.B. dem Energiewirtschaftsgesetz (EnWG) und dem Telekommunikationsgesetz (TKG) flankiert. Auf europäischer Ebene kommen die Richtlinien NIS 2 (Directive on security of network and information systems) und RCE (Directive on the resilience of critical entities) dazu.

Zur Umsetzung der NIS-2-Richtlinie, die sich mit der Cybersicherheit von kritischen Infrastrukturen befasst, gibt es bereits einen Referentenentwurf (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG). Hier kommen viele Veränderungen auf die Organisation zu. Die wichtigsten sind unter anderem die folgenden:

- **Ausweitung des Anwendungsbereichs:** Die Anzahl der Organisationen, die von den Regelungen betroffen sind, steigt stetig. Schon NIS 2 sieht eine deutliche Erweiterung des Anwendungsbereichs vor. Der Referentenentwurf des Bundesinnenministeriums lässt erwarten, dass der deutsche Gesetzgeber sogar noch weiter geht, als es von NIS 2 gefordert wurde. Die Regelungen dazu sind teilweise sehr komplex. Zu den Schwellenwerten will die Bundesregierung eine weitere Verordnung erlassen, die dann sowohl für die Cybersicherheit (NIS 2 und BSIG), als auch für die physische Sicherheit (RCE und KRITIS-Dachgesetz) gelten soll. Wie soll das in der

Realität umgesetzt werden?

- **Governance und Organhaftung:** NIS 2 sieht vor, dass Vorstände, Geschäftsführung etc. für die Überwachung der Umsetzung der Risikomanagementmaßnahmen Sorge tragen sollen und fordert, dass ein Verstoß gegen diese Pflicht zur privaten Haftung führt. Diese Vorgaben scheint die Bundesregierung besonders streng umsetzen zu wollen. Der Referentenentwurf sieht vor, dass die Leitungsorgane ihren Verpflichtungen persönlich nachkommen müssen. Außerdem sollen sie gegenüber ihrer Organisation auch für Bußgelder haften, die aufgrund ihrer Pflichtverletzungen verhängt wurden. Dies kann insbesondere für Vorstände und Geschäftsführer von großen Unternehmen fatale Folgen haben.

  Denn die Obergrenze für Bußgelder wird von bisher 20 Millionen Euro (§ 14 Abs. 5 BSIG i.V.m. § 30 Abs. 2 Satz 3 OWiG) teilweise auf 2 % des globalen Jahresumsatzes des Unternehmens erhöht. Da vorgesehen ist, dass die Organisationen auf die Ersatzansprüche gegenüber den Leitungsorganen nicht verzichten dürfen, sind die neuen Haftungsregeln für Leitungsorgane potenziell existenzgefährdend.

Kritische Infrastrukturen

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

1. Energie
2. Informationstechnik und Telekommunikation (Rechenzentren)
3. Transport und Verkehr
4. Gesundheit
5. Medien und Kultur
6. Wasser
7. Ernährung
8. Finanz- und Versicherungswesen
9. Siedlungsabfallentsorgung
10. Staat und Verwaltung

Doch wie gehen all diese Organisationen und Unternehmen mit diesem Thema um? Wie sollen oder können Unternehmen Ihre bestehende IT-Infrastruktur auf NIS2 konforme Lösungen kurzfristig übertragen?

Kommunen, die Verwaltung sowie Medien und Kultur unterliegen nicht der Regulierung durch das BSIG. Sind z.B. Kommunen weniger gefährdet? Natürlich nicht!

Was bedeuten all diese Regelung auf der technischen Ebene, was kann umgesetzt werden?

1. **Die Anforderungen an die Netzwerkinfrastruktur steigen überdurchschnittlich.** Eine Vielzahl von Soft- und Hardwarekomponenten müssen miteinander funktionieren, verwaltet und gepflegt werden. Das erhöht die Komplexität massiv, die Administrations-, Anschaffungs- und Wartungskosten steigen. Und damit nehmen die Anfälligkeit, Sicherheitslücken und Ausfälle stark zu.

2. **Die Arbeitswelt im Wandel.** Nicht nur die Geschäftsleitung auch Mitarbeiter arbeiten im Büro, unterwegs und von zu Hause. Sie arbeiten mit Endgeräten in Fremdnetzwerken mit lokal

installierten, remote bereitgestellten oder auf cloudbasierten Anwendungen. Wie sollen all diese Netzwerke isoliert oder das Arbeiten außerhalb des eigenen Netzwerkes gesichert werden?

3. **KI lernt „Laufen“** und das, was die KI heute kann, ist erst der Anfang. Cyberkriminelle perfektionieren mit Hilfe der KI ihre Methoden und können KI unterstützt Angriffe ausführen.

Die Aufrechthaltung der IT-Sicherheit bleibt schwierig. IT - Verantwortliche müssen UMDENKEN. Überall sicher arbeiten und gleichzeitig die Business Continuity aufrechterhalten, ist mit erheblich hohem Aufwand verbunden - aber möglich!

Wie die jüngsten Berichte belegen, kämpfen sogar Unternehmen, die viel Geld in Hard-, Software und Personal investiert haben mit der Zerbrechlichkeit ihrer Netzwerkinfrastruktur. Politisch und wirtschaftlich motivierte Cyberkriminelle erlangen Oberhand über Daten und Systeme bewirken Schäden in Milliardenhöhe.

sayTEC bietet ein ganzheitliches NIS2 konformes Sicherheitskonzept für Städte, Kommunen und Unternehmen an. Sie umfasst die gesamte IT-Infrastruktur - bestehend aus einer hyperkonvergenten Serverstruktur, Storage, Backup und einer einzigartigen Zero Trust Client Access Lösung für die Netzwerksicherheit. Sie bilden drei ineinandergreifende und miteinander wirkende Sicherheitsbereiche. Also drei Tresore in einem Tresor. Die **ganzheitliche und NIS2 konforme Lösung** erschließt alle relevanten Anforderungen und reduziert die Komplexität um bis zu 70%. Die Risiken werden deutlich minimiert und eine unterbrechungsfreie Plattform zur Sicherung der Business Continuity bereitgestellt.

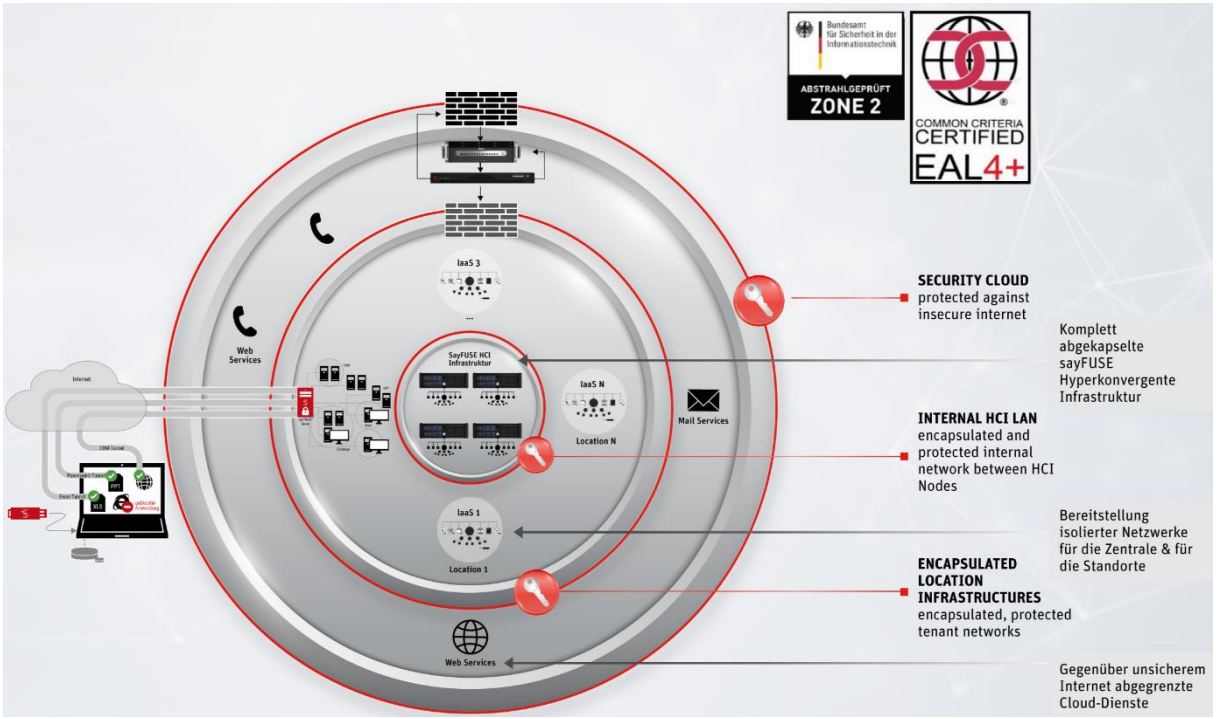
Die Lösung – das Sicherheitskonzept der sayTEC AG

Die sayTEC Lösung schützt nachhaltig gegen Cyberangriffe, sichert maximale Verfügbarkeit und Beständigkeit. Das Risiko erfolgreich angegriffen zu werden geht fast gegen null und Hard- und Software-Ausfälle gehören der Vergangenheit.

Das Sicherheitskonzept besteht aus drei Sicherheitszonen und drei Technologien.

Der **erste und innerste** bildet den isolierten Kern und beherbergt die gesamte IT-Infrastruktur mit allen erforderlichen Komponenten. Betrieben wird dieser Bereich **mit drei Technologien: Die sayFUSE HCI, sayFUSE Highspeed Backup und die sayTRUST VPSC Zero Trust Technologie**. So wird eine hyperkonvergente Infrastruktur mit allen Diensten durch sayFUSE HCI All-in-One Appliances, Datensicherung sowie die hochsichere Kommunikation bereitgestellt.

- Firewall
- Router
- Loadbalancer
- Kubernetes
- VPN
- Floating-IP
- Virtuelle Server
- Virtuelle Anwender-PC
- Mehrstufiges Backup
- Applikation Veröffentlichung
- NFS-, iSCSI-, S3-Storage
- Single Sign-on
- Personal Key Identifikation
- Spurenlose ZeroTrust Kommunikation
- Backup

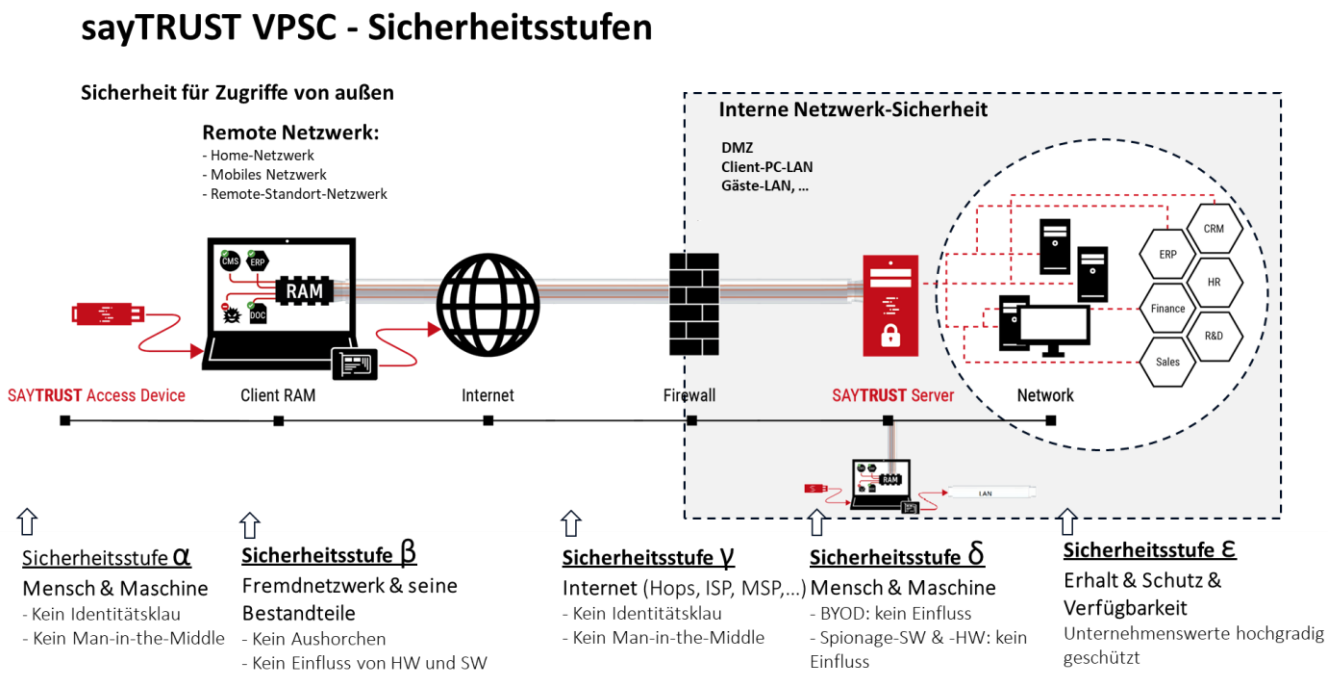


Das System ist fehlertolerant gegenüber Komplettausfällen und ermöglicht einen unterbrechungsfreien Betrieb.

Die **sayFUSE Backup Technologie** für Sicherung, Wiederherstellung, Archivierung und Auslagerung übernimmt die Hochgeschwindigkeits-Backup-Aufgaben (bis zu 12 TB/Stunde). Diese Technologie übernimmt die Funktion der Versicherung für Daten und Unternehmenswerte.

Der zweite Sicherheitsbereich ist der Bereich der kritischen Netzwerke. Hier werden alle Services für ein oder mehrere Standorte zur Verfügung gestellt. Die Zeit, wo Unternehmen an jedem Standort IT-Systeme betreiben, ist vorbei. Das gilt auch für Ministerien oder Organisationen mit mehreren Standorten.

Alle erforderlichen Dienste von einer Zentrale zur Verfügung stellen, ist mit der sayTRUST VPSC Zero Trust Client Access Technologie möglich. Sie ermöglicht den hochsicheren und nicht sichtbaren Zugriff der Anwender auf einzelne Anwendungen, Dienste, Netzwerke oder den eigenen Arbeitsplatz-Computer nach Überprüfung der persönlichen und systembedingten Identität über mehrstufige, ineinandergreifende und sich gegenseitig bedingende Sicherheitsverfahren. Die sayTRUST VPSC ermöglicht eine hochsichere Kommunikation durch das Ineinandergreifen unterschiedlicher Sicherheitselemente über die gesamte Kommunikationsstrecke und das Beseitigen aller Schwachstellen an den Schnittstellen. Eine Sicherheitslösung, die mit der persönlichen Identifizierung des Anwenders und seines PC´s, über die gesamte Kommunikationsstrecke und auch innerhalb des zu schützenden Netzwerks nichts zulässt, was nicht überprüft wurde.



Während bei herkömmlichen VPN-Lösungen immer ein Kompromiss eingegangen wird, vereint sayTRUST VPSC hohe Sicherheit und einfache Bedienung miteinander.

Sicherheit darf keinerlei Kompromisse zulassen - aber gleichzeitig muss auch für einen unerfahrenen Anwender die Bedienung einfach sein. Der Anwender steckt sein persönliches Token an ein beliebiges PC, identifiziert sich und arbeitet.

Im Hintergrund steuert der Kommunikationsclient über Black- und White Listen, das Tunneln, Blockieren und Isolieren von Anwendungen auf dem Anwenderrechner und auch innerhalb des zu schützenden Netzwerks.

Bei der sayTRUST VPSC – Zero Trust Client Access Lösung beginnt die Sicherheit bereits vor dem Kommunikationsaufbau. Die integrierte PKI sorgt dafür, dass ausschließlich berechtigte Nutzer, nach Prüfung der Identität (Biometrie, PIN), die Kommunikation starten kann. Unberechtigte Personen und PCs sehen nichts, haben kein Zugriff.
Die achtstufige Defence-in-Depth Layer 7 Kommunikation mit personifiziertem Perfect-Forward-Secrecy-Schlüssel erfolgt verschlüsselt aus dem RAM des Anwenderrechners heraus. So wird, im Gegensatz zu den klassischen Lösungen, eine Schadanwendung bereits im Ursprung der Kommunikation - am Eingang des Tunnels - erkannt und abgewehrt.

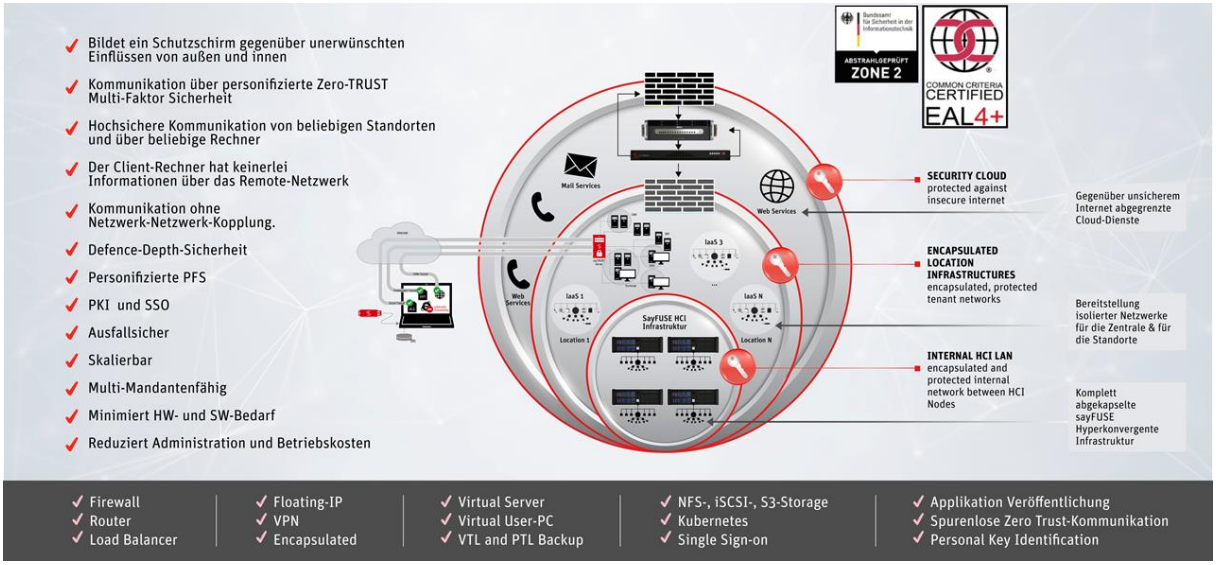
Auf dem Rechner des Anwenders ist keine Installation und auch keine virtuelle Netzwerkkarte erforderlich. Es werden keine Informationen und keine IP-Adressen aus dem zu schützenden Netzwerk benötigt. Von außen sind das Netzwerk und die dazugehörigen Informationen unsichtbar. Heimtückisch von Hackern verwendete Techniken, Sniffing um in Echtzeit Daten zu erfassen bleibt auch auf dem Client-PC erfolglos. Die Verbindung bleibt unsichtbar.

Für den Anwender ist besonders angenehm, dass er seine Arbeitsumgebung als Plug-and-Play Lösung in Form des sayTRUST Secure Access Token immer bei sich hat und überall an jedem beliebigem PC hochsicher arbeiten kann.

Diese drei Standbeine bilden eine beliebig skalierbare, ausfallfreie Hochsicherheitsinfrastruktur. Sie schützen die Unternehmenswerte gegen Cyberangriffe und Katastrophenfälle, gewährleisten Business Continuity und damit die Aufrechterhaltung der Betriebsfähigkeit.

Weitere Vorteile für Nutzer ist die hohe Investitionssicherheit
Es ist keine zusätzliche Hard- und Software für die Standorte erforderlich:

- Server ➔ enthält eine unlimitierte Anzahl von virtuellen Servern
- Storage ➔ enthält Block-, iSCSI, NFS- und S3-Object-Storage
- Arbeits-PC/Notebook (VDI) ➔ enthält eine unlimitierte Anzahl von virtuellen Client PCs
- Load Balancer ➔ enthält eine beliebige Anzahl von Lastenausgleichsservern
- Firewall ➔ enthält eine beliebige Anzahl von FWs
- Zero Trust Client Access ➔ enthält je Standort einen sayTRUST VPSC-Server
- PKI ➔ in sayTRUST integriert
- SSO ➔ in sayTRUST integriert
- Backup Server ➔ enthält sayFUSE Backup für VTL und PTL mit Medienbruch und Backup Storage Auslagerung



All-in-One Module geben maximale Flexibilität und Skalierbarkeit für gegenwärtige und zukünftige Anforderungen. Die modulare Lösung reduziert die Komplexität und laufende Betriebskosten sowie den Energieverbrauch und damit CO_2-Ausstoßes.

Die ganzheitliche IT-Infrastrukturlösung baut einen Schutzschirm gegenüber unerwünschten Einflüssen von außen und von innen auf und stellt die Verfügbarkeit und Skalierbarkeit sicher.

Kontakt:

sayTEC AG
Bremer Straße 11
80807 München
E-Mail: kontakt@saytec.eu

SAYTEC