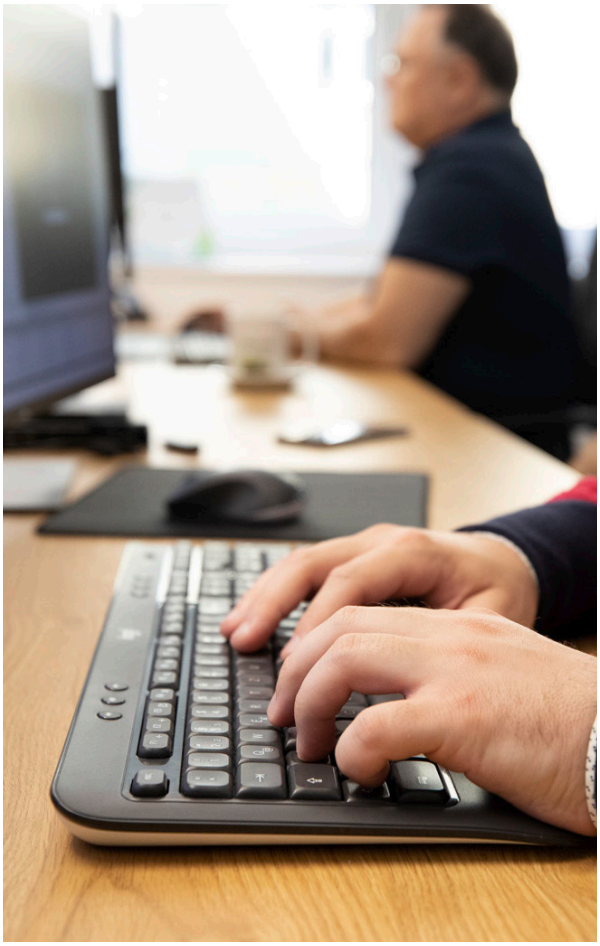
HXS
Die IT Xperten für Ihr Business.

Network Access Control von HXS:
Wirkungsvolle und flexible Security für Ihren Netzwerkzugang

HXS NAC: Ein essentielles Element in der Welt der Managed Solutions von HXS, das Sie effizient im operativen Alltag Ihrer IT-Infrastruktur unterstützt. Die passende HXS NAC Lösung für Ihr Unternehmen gibt Ihnen die beruhigende Gewissheit, dass die erfahrenen Security-Experten von HXS rund um die Uhr die Zutrittssicherheit zu Ihrem Netzwerk überwachen. Diese 24/7-Überwachung ermöglicht uns den lückenlosen Überblick über alle befugten und unbefugten Zutritte – verdächtige Aktionen können so schnell erkannt und die entsprechenden Gegenmaßnahmen rechtzeitig eingeleitet werden.

Warum HXS NAC gerade jetzt so wichtig ist? Unternehmensnetzwerke sind in Zeiten von Mobile Office und „Bring Your Own Device“ immer häufiger von Zugriffen durch unautorisierte oder fremde Endgeräte bedroht. Eine Tatsache, die durch die Corona-Krise noch verschärft wurde: Die Häufigkeit von Cyberattacken wie z. B. Ransomware oder Phishing hat während der COVID-19-Krise drastisch zugenommen und bedeutet auch in Zukunft eine wachsende Gefahr für Ihre Unternehmens-IT.

HXS NAC bietet als zuverlässiger Torwächter die wirkungsvolle Gegenstrategie und schützt Ihr Netz effizient und flexibel vor unbefugten Fremdzugriffen und eingeschleuster Schadsoftware wie z. B. Viren oder Würmer. Dabei schafft HXS NAC nicht nur maximale Sicherheit, sondern auch Transparenz und Nachvollziehbarkeit, indem das System spielend den Überblick über die Vielzahl der Netzwerkteilnehmer behält. Damit ist HXS NAC die passende Ergänzung für jedes moderne Security Portfolio und steigert die Sicherheit ihres Netzwerkes entscheidend.



Entscheiden Sie sich deshalb jetzt für HXS NAC und legen Sie Ihre Netzwerk-Security in erfahrene Expertenhände – und das besonders wirtschaftlich und zum monatlichen Fixpreis.

Selbstverständlich ist HXS NAC nur eines von vielen Elementen einer umfassenden Netzwerk-Security-Strategie und erweitert wichtige Security- Elemente wie Firewall, WLAN-Security, Datensicherung und vieles mehr um einen neuen und heute umso aktuelleren Punkt. Informieren Sie sich deshalb jetzt über die vielfältigen neuen Risiken, die modernen Unternehmens-Netzwerken bei ungenügender Zugangssicherung drohen – und setzen Sie zuverlässig wirkungsvolle Gegenmaßnahmen gegen Cyberangriffe von außen und innen mit HXS NAC. Ihre erfahrenen HXS Security Xperten beraten Sie dazu gerne in einem ausführlichen persönlichen Gespräch.

Ihre Vorteile mit HXS NAC:

- Führende IT Security-Technologie
- Problemlose Einbindung auch in heterogene Infrastrukturen
- Schutz vor unautorisiertem Zugriff von innen
- Keine Netzwerkverbindung für Unbefugte
- Sicherheit vor Fremdgeräten
- Zuverlässige Geräteerkennung

Führende Security-Technologie

HXS NAC basiert auf der extrem flexiblen und effizienten High-End- Sicherheitssoftware des führenden deutschen Netzwerk-Securityanbieters macmon. macmon wurde als erster NAC-Anbieter mit dem BSI-Zertifikat des deutschen Bundesamts für Sicherheit in der Informationstechnik ausgezeichnet. Damit setzen wir auf einen der besten Security-Software-Partner weltweit – und bieten Ihnen gemeinsam mit dem hochkarätigen HXS-Expertenwissen bei Implementierung und Betrieb das Optimum an Sicherheit für Ihre Unternehmens-IT.

Problemlose Einbindung auch in heterogene Infrastrukturen
macmon ist einer führenden Pioniere unter den Network Access Control- Anbietern mit einer besonders hohen Kundenzufriedenheit von 95 %. Führende internationale und nationale Unternehmen und Institutionen wie z. B. die Volkswagen Stiftung oder das deutsche Bundesministerium für Justiz vertrauen auf macmon-basierte NAC-Lösungen. Das besondere Know-how von macmon bei einer großen Vielzahl an Unternehmensanwendungen in den unterschiedlichsten Branchen und Dimensionen ermöglicht z. B. die problemlose Einbindung einer großen Vielzahl an Bestandsswitches von unterschiedlichen Herstellern ebenso wie die Einbindung in heterogene Netzwerk-Infrastrukturen.

Keine Netzwerkverbindung für Unbefugte
Eine der wichtigsten Funktionen eines effizienten NAC-Systems: Es verhindert zuverlässig, dass Unbefugte eine gültige Netzwerk-Verbindung erhalten. Dies ist vor allem deshalb wichtig, da die Netzwerklandschaften in größeren Unternehmen – aber z. B. auch im öffentlichen Bereich – immer heterogener werden: Eine Vielzahl an unterschiedlichen Endgeräten möchte auf das Netzwerk zugreifen. Das können neben unternehmenseigenen, autorisierten Geräten z. B. auch immer häufiger für die Arbeit erforderliche (und durch das NAC-System entsprechend kontrollierte) Privatgeräte von Mitarbeitern sein – oder auch unautorisierte Privatgeräte und insbesondere Geräte von Besuchern und Unternehmensfremden. Ein wirkungsvolles NAC-System erkennt präzise den Unterschied – und schaltet Risiken sofort aus, ehe sie zur Gefahr werden können.

Kein unautorisierter Zugriff von innen
Nicht nur Angreifer von außen, auch der unautorisierte Zugriff von innen kann eine große Gefahr für Ihr Unternehmens-Netzwerk bedeuten: durch das unerwünschte Einloggen von betriebsfremden Personen oder die Verbindung mit unerwünschten Geräten kann schnell Schadsoftware wie z. B. Viren oder Würmer ins System gelangen. Effizientes Netzwerk-Security- Management berücksichtigt daher auch diese empfindlichen und oft vernachlässigten Sicherheitslücken – denn der beste Schutz nach außen nützt nichts, wenn interne Risiken übersehen werden.

Sicherheit vor Fremdgeräten
Home Office und ortsunabhängiges, flexibles Arbeiten sind spätestens seit der Corona-Krise zu wichtigen Faktoren des modernen Arbeitslebens geworden. Damit wird auch das „Bring Your Own Device"-Prinzip immer populärer, das Mitarbeitern ebenso wie Unternehmen entscheidende Vorteile bringen kann. Das große Risiko dabei: mit dem immer höheren Anteil von Privatgeräten im Unternehmensnetzwerk ist auch das Risiko von problematischen Systemzugriffen stark gewachsen.

Auch der wachsende Trend des „Internet of Things" sorgt für eine immer größere Flut an netzwerkfähigen Geräten – und damit für ein immer höheres Risiko von unerwünschten Teilnehmern im Netz. Der Netzzugriff durch eine große Zahl an Fremdgeräten zählt speziell in Branchen wie dem Handel, dem Dienstleistungssektor, der Gastronomie und Hotellerie sowie in vielen anderen Branchen mit hoher Kundenfrequenz mittlerweile zum Alltag.

Durch diese nicht autorisierten Geräte kann unwissentlich oder auch wissentlich Schadsoftware ins System eingeschleust werden – oder gar der unerlaubte oder missbräuchliche Zugriff auf sensible Daten erfolgen. Hier sorgt HXS NAC als schnelle, vollautomatisierte Zugangskontrolle zuverlässig dafür, dass nur kontrollierte und zulässige Geräte Zugriff auf das Netzwerk erhalten. Betriebsfremde und unbefugte Geräte werden hingegen sofort identifiziert und ihr Netzwerkzugang konsequent unterbunden.

Zuverlässige Geräteerkennung
Jedes NAC-System ist nur so wirkungsvoll wie wie seine zuverlässige und detaillierte Unterscheidung von autorisierten und nicht-autorisierte Geräten. Ehe ein Endgerät im Netz kommunizieren kann, prüft HXS NAC deshalb nicht nur vollautomatisiert, ob eine Autorisierung vorliegt. HXS NAC kontrolliert darüber hinaus auch nach einem klar und individuell konfigurierbaren System an Richtlinien jedes mögliche Detail-Risiko eines Endgeräts – z. B., ob der installierte Virenscanner aktuell ist oder ob das Betriebssystem die neuesten Sicherheits-Updates aufweist. Nur, wenn sämtlichen definierten Sicherheitsrichtlinien erfüllt sind, erhält das Endgerät Zugriff auf das Netzwerk und daran angeschlossene Ressourcen.

Bei Geräten, die den definierten Vorgaben nicht entsprechen, erteilt HXS NAC je nach Risiko entweder eine komplette oder teilweise Sperre der Netzwerkverbindung. So kann beispielsweise ein privates Mitarbeiter-Gerät ohne aktuelle Security-Updates vorübergehend in einem speziellen Quarantänenetz isoliert werden, das lediglich den Zugriff ins Internet, aber nicht ins Unternehmensnetzwerk erlaubt. Dort kann das Gerät mit aktuellen Updates versorgt werden, bis es wieder den geltenden Sicherheitsrichtlinien entspricht und vollen Netzwerkzugriff erhält. Die Geräteerkennung kann hierbei auf diversen Security-Faktoren basieren: entweder auf Basis der MAC-Adresse, auf Basis einer Authentifizierung mittels Radius per Username und Passwort oder durch Zertifikats- Authentifzierung, die eine Public-Key-Infrastruktur (PKI) voraussetzt.