macmon®

Leitfaden

Best Practice zum Schutz von Innentätern

Inhalt

- Warum Network Access Control-Lösungen (NAC)?
- Typische Stolpersteine bei der internen IT-Sicherheit
- 10 Tipps für die Planung von NAC-Projekten
- Selbstcheck des Schutzes vor Innentätern

■Warum Network Access Control-Lösungen (NAC)?

Die Zugangskontrolle ist zu einem zentralen Thema für den sicheren Betrieb von Unternehmensnetzwerken geworden. Der Anschluss eines nicht zugelassenen Computers an das Netzwerk eines Unternehmens kann in den meisten Fällen weder verhindert noch erkannt werden. Mit einem unautorisierten Anschluss ist zwar weder die Teilnahme an der Netzwerkkommunikation noch ein Zugriff auf Ressourcen im ersten Schritt möglich, doch können diese Rechte durch einen internen Angriff auf die Infrastruktur des Netzwerks erzwungen werden. Deshalb sind Network Access Control-Lösungen (NAC) erforderlich, die vorformulierte Sicherheitsregeln und präkonfigurierte Netzelemente zur Steuerung des Netzzugangs enthalten.

Hintergrund dieser kräftigen Entwicklung ist nicht zuletzt, dass die Unternehmen und auch Behörden zunehmend Personen ohne Mitarbeiterstatus Zugang zum Netzwerk einräumen müssen. Dies können mobil arbeitende Mitarbeiter von Dienstleistungspartnern, Beratern oder Zulieferer bzw. auch Kunden sein. Häufig sind Notebook-Zugänge für Gäste in den Unternehmen möglich, ohne dass die Geräte bisher ausreichend auf Gefahren wie Viren oder Datendiebstahl geprüft werden. Für diese Nutzergruppen gilt es Regeln zu entwickeln, etwa auf welche Systeme sie Zugriff erhalten. Außerdem gehen weitere Gefahren gehen von mobilen Rechnern aus, die sowohl im Firmen-LAN als auch an nicht vertrauenswürdigen Internetzugangspunkten eingesetzt werden.

Noch aus einer anderen Richtung wird der deutlich wachsende Bedarf an NAC-Lösungen genährt: die steigenden Compliance-Anforderungen in den Unternehmen. Sie erzeugen allein aus rechtlichen die Notwendigkeit verstärkter Maßnahmen für eine transparente und revisionssichere Steuerung des Netzwerkszugangs. Allerdings gibt es auch NAC-Lösungen, die einen Umbau der Netzwerkarchitektur erfordern, hohe Anpassungskosten verursachen und sehr zeitaufwändig sind.

Eigene Bemerkungen: _____

_____

_____

_____

■Typische Stolpersteine bei der internen IT-Sicherheit

Zwar hat sich den letzten drei Jahren die Zahl der realisierten Network Access Control-Lösungen (NAC) zum Schutz vor internem Datenmissbrauch mehr als verdoppelt. Trotzdem verfügen nach einer Vergleichserhebung der macmon secure gmbh erst zwei von fünf Firmen über einen solchen Schutz der Netzwerkzugänge. Die Consultants des NAC-Softwarehauses haben aus Praxissicht die Gründe für die Zurückhaltung untersucht und einige der weit verbreiteten Stolpersteine zusammengestellt:

Projekte zum Schutz vor externen Angriffen haben immer Vorrang: Zweifellos sind Attacken und Manipulationsversuche über das Internet eine kontinuierliche Gefahr auf gleichbleibend hohem Niveau. Studien zeigen aber wiederholt, dass beim Schutz vor Datendiebstahl eine besondere Gefahr vor Innentätern ausgeht. Diesem Sachverhalt wird in den Security-Investitionen meist zu wenig Rechnung getragen, weil der Fokus fast ausschließlich auf die externen und öffentlich populär diskutierten Gefahren gerichtet wird.

Zu isolierte Impulse: Obwohl die IT-Sicherheit unwidersprochen ein unternehmensweites Thema darstellt, obliegt sie fast ausschließlich der IT oder den Security-Verantwortlichen. Diese funktionale Zuordnung macht zwar in fachlicher Hinsicht Sinn, darf aber nicht so weit gehen, dass die Business-Abteilungen von einem eigenen Engagement befreit werden. Dies ist jedoch in der Praxis weit verbreitet zu beobachten. Als Konsequenz fehlt es den Initiatoren von Maßnahmen an Unterstützung und können mögliche Optimierungspotenziale in der IT-Sicherheit nicht ausreichend aktiviert werden.

Wirtschaftliche Nutzeneffekte werden nicht gesehen: Investitionen in Sicherheitssysteme begründen sich im Regelfall mit der Abwehr von Gefahren, ohne dass ein Zusatznutzen erwartet wird. Im Falle der NAC-Lösungen (Network Access Control) zum Schutz vor internen Datenmissbrauch stellt sich die Situation jedoch anders dar, weil diese Systeme auch gleichzeitig zur Steuerung des Energieverbrauchs aller Netzwerkkomponenten eingesetzt werden können. Dies bewirkt einen ROI der NAC-Investition bereits im ersten Jahr. Solche Effekte werden in den Unternehmen jedoch nicht deutlich, weil die Verantwortlichen für die IT-Sicherheit einerseits und die Energiekosten andererseits hierzu nicht miteinander kommunizieren.

Keine wirkungsvolle Security-Führung: Weil die IT-Sicherheit in der Realität der Unternehmen keine oder nur eine geringe strategische Bedeutung hat, fehlt es den Security-Verantwortlichen an der notwendigen Durchsetzungskraft. Statt IT-Sicherheit als eine rein operative Funktion zu verstehen bedarf es einer vom Top-Management unterstützten Roadmap. Sie muss explizit auch den internen Schutz von Datenmissbrauch beinhalten, in ihren sicherheitsstrategischen Zielen mittelfristig angelegt sein und gleichzeitig die Unterstützungspflichten durch die gesamten Organisationseinheiten klären.

Angst vor hohem Projektaufwand: Entgegen einer weit verbreiteten Annahme sind NAC-Lösungen typischerweise so angelegt, dass sie eine zeitaufwändige Projektrealisierung vermeiden. Dadurch lassen sich Implementierungen bereits in wenigen Stunden vornehmen. Auch für eine flexible Skalierung des Security-Systems gilt dies. Voraussetzung einer schnellen Implementierung ist die konzeptionelle Ausrichtung der Lösung als Management-Tool, das technisch nicht in die bestehende Infrastruktur integriert werden muss.

Es wird mit fehlenden Administrationsressourcen argumentiert: Der Hinweis auf den Betreuungsaufwand resultiert vornehmlich aus Erfahrungen mit Managementtools aus anderen Funktionsbereichen, geht aber im Falle von NAC-Lösungen im Regelfall an den realen Gegebenheiten vorbei. Vielmehr sind sie ähnlich ihrer aufwandsarmen Implementierung so angelegt, dass lediglich ein unbedeutender Administrationsbedarf entsteht und somit die IT-Ressourcen nicht nennenswert belastet werden.

Beschränktes Augenmerk auf die klassischen mobilen Geräte: Fast alle Mitarbeiter und Personen mit Zutritt zu den Betriebsräumen tragen heutzutage Handys mit sich, teilweise auch andere Mobile Devices mit Speicherfunktionen. Dabei verfügen typische Mobiltelefone heutzutage über ein beträchtliches Speichervolumen, so dass damit bei fehlenden NAC-Lösungen potenziell umfassende Daten widerrechtlich herunter geladen werden können.

Der Irrglaube, Angriffe zielen nur auf die großen Namen ab: Letztlich besitzt jedes Unternehmen eine Menge schützenswertes Know-how, auch die kleineren Betriebe. Denn gerade mittelständische Firmen zeigen meist eine große Innovationskraft, entwickeln kontinuierlich Produktneuheiten und haben deshalb eine große

Anziehungskraft für wirtschaftskriminelle Aktivitäten. Insofern droht auch ihnen im Falle des Verlustes von Informationen ein erheblicher Schaden.

Angst vor Transparenz: NAC-Systeme bilden über das Live-Monitoring und Bestandsmanagement die gesamte Gerätelandschaft ab innerhalb der Netzwerk-Infrastruktur ab. Somit würden dann auch alle Schwächen ans Tageslicht befördert, für deren Beseitigung möglicherweise keine Ressourcen bestehen. Deshalb wird trotz erkannter Notwendigkeit die Einführung einer NAC-Lösung gerne ohne feste zeitliche Planung in die Zukunft verschoben.

Eigene Bemerkungen: _____

_____

_____

_____

■10 Tipps für die Planung von NAC-Projekten

Allein schon weil zunehmend Personen aus dem Kunden-, Lieferanten- und Partnerkreis Zugang zu den internen Netzwerken gewährt werden muss, spielt die Kontrolle der Netzwerkzugänge inzwischen eine zentrale Bedeutung in den Sicherheitskonzepten der Unternehmen. Zudem werden vermehrt mobile Endgeräte wie Laptop, Smartphone und iPad im Unternehmensnetz eingesetzt. „NAC-Lösungen gehören deshalb inzwischen zum Pflichtprogramm, weil ansonsten ein erheblicher Schaden etwa durch Datendiebstahl entstehen kann“, urteilt Christian Bücker, Geschäftsführer der macmon secure gmbh. Er verweist auf die immer wiederkehrenden Fälle mit öffentlich bekannt gewordenem Datenmissbrauch und dessen häufig erheblichen Konsequenzen. „Dieses Risiko betrifft aber keineswegs nur prominente sondern praktisch jedes Unternehmen.“

Gleichzeitig gibt Bücker zu bedenken, dass sich viele Firmen noch am Einsatz von Netzwerke Access Control-Lösungen (NAC) vorbeigemogelt haben. „Dies liegt nach unseren Beobachtungen nicht an der fehlenden Erkenntnis, dass sie notwendig sind, sondern weil sie angesichts enger personeller Ressourcen den Planungsaufwand scheuen.“ macmon secure hat deshalb produktneutrale Planungstipps erarbeitet:

1. **Ziele definieren:** Es gilt die Frage zu klären, was mit der NAC-Lösung erreicht werden soll. Dazu gehören typischerweise der Schutz sowohl vor Fremdgeräten als auch vor unsicheren Geräten, etwa mit nicht ausreichendem Virenschutz. Aber auch die Verhinderung von ungesteuerten Gerätebewegungen und die gezielte Bereitstellung von Netzwerkrechten für Gäste, Drucker, Notebooks, Telefone und andere Netzwerkkomponenten sind üblicherweise darin einzubeziehen.
2. **Authentisierungsverfahren bestimmen:** Erforderlich ist eine Geräte-Authentifizierung beim Netzwerkzugang. Diese kann proprietär oder über 802.1X erfolgen, und sie kann auch auf verschiedenen Sicherheitslevels abhängig von den Endgeräten und den Sicherheitsanforderungen angeboten werden. Über die MAC-Adresse, Protokoll-Profile (Footprints) oder Geräte-Profile (Fingerprint), Anmeldeinformationen, Zertifikate bis hin zu stark kryptografischen Verfahren mit Chip-Karten oder dem TPM-Chip
3. **Seiteneffekte mitnehmen:** Die vom NAC-System durchgeführte Endgeräte-Identifizierung bietet auch eine Vielzahl von Möglichkeiten, organisatorische Abläufe zu verbessern. Beispielsweise wird das Bestandsmanagement durch Live-Daten zur Lokalisierung der Geräte und zur Erkennung nicht genutzter Geräte aufgewertet. Nicht genutzte Switch-Ports werden zur Verbesserung der

Kapazitätsplanung oder zur Begleitung von Umzügen angezeigt usw. Darüber hinaus besteht die Möglichkeit, durch ein bedarfsgerechtes Ein- und Ausschalten der PC-Arbeitsplätze Energiekosten zu sparen.

4. **Ergänzende Analysen:** Vorteilhaft sind Methoden und Techniken, die beim Netzwerkzugang spezielle Gerätetypen (z.B. Drucker, IP-Telefon etc.) automatisch erkennen.
5. **Dienste Zugriffe beschränken:** Es sollte mittels VLAN-Steuerung eine logische Trennung des Netzes erfolgen, damit Benutzer nicht auf alle Dienste zugreifen können.
6. **Nutzungszeit begrenzen:** Die Zugänge für Unternehmensgäste sollten mit einer restriktiven zeitlichen Beschränkung versehen werden.
7. **Angriffe erkennen und verhindern:** Die Überwachung des Netzwerkes sollte auch Man-in-the-middle-Angriffe wie durch ARP-Poisoning oder MAC-Flooding erkennen und verhindern.
8. **Erweiterten Schutz realisieren:** Durch die Integration von verschiedenen Sicherheitssystemen (z. B. Firewall, Virenschutz, IDS/IPS, VPN usw.) über proprietäre Schnittstellen (API, CLI) oder standardisierte Verfahren (IF-MAP) können Bedrohungen früher erkannt und wirkungsvoller bekämpft werden. Das NAC-System spielt in so einer Kombination immer eine zentrale Rolle, da es den Angreifer oder das bedrohende System unmittelbar vom Netzwerk trennen kann.
9. **Monitoring der Richtlinieneinhaltung:** Unbedingt zu empfehlen ist im Bereiche der Clients und insbesondere der mobilen Clients eine Überwachung der Einhaltung der Sicherheitsrichtlinien wie Virenschutz, Patchmanagement, Sicherheitskonfigurationen etc.
10. **Reaktionen automatisieren:** Sicherheit darf nicht von Fall zu Fall entschieden werden und auch nicht von der Auslastung der Administration abhängen. Darum sollten klare Regeln für den Umgang mit Fremdsystemen, nicht sicheren Systemen, das Verhalten bei nicht gemeldeten Umzügen etc. festgelegt und aktiviert werden.

Eigene Bemerkungen: _____

_____

_____

■Selbstcheck des Schutzes vor Innentätern

Die nachfolgenden Fragen zur Selbstanalyse dienen einer tendenziellen Bewertung der individuellen Ist-Bedingungen. Je zahlreicher es dabei zu Nein-Nennungen kommt, desto deutlicher zeichnet sich das Erfordernis ab, adäquate Maßnahmen zur Optimierung der internen IT-Sicherheit vorzunehmen.

	□Ja	□Nein
▪ Bestehen verbindliche Regeln zur internen Informationssicherheit?	❑	❑
▪ Sind alle sicherheitsrelevanten Policies technisch umgesetzt?	❑	❑
▪ Werden in festem Rhythmus und systematisch Risikoanalysen zur Informationssicherheit durchgeführt?	❑	❑
▪ Können Verletzungen gegen die Sicherheitsvorschriften detailliert festgestellt werden?	❑	❑
▪ Sind Security und Administration organisatorisch getrennt?	❑	❑
▪ Sind in bestehenden Dienstleistungsverträgen Sicherheitsmaßnahmen und -verfahren berücksichtigt?	❑	❑
▪ Gibt es in Ihrem Unternehmen eine Inventarisierung, die alle wichtigen Informationswerte enthält?	❑	❑
▪ Sind diese Informationswerte nach ihrem Schutzbedarf definiert?	❑	❑
▪ Bestehen für die eigenen Mitarbeiter verbindliche Vertraulichkeits-vereinbarungen?	❑	❑
▪ Sind in den Verträgen mit Geschäftspartnern überprüfbare Datenschutzregeln enthalten?	❑	❑
▪ Gibt es festgelegte Regeln, nach denen Art, Umfang und Kosten von Sicherheitsvorfällen quantitativ erfasst werden?	❑	❑
▪ Gibt es ein Genehmigungsverfahren für die Mitnahme von IT-Systemen / Software / Informationen aus den Geschäftsräumen?	❑	❑
▪ Gibt es dokumentierte Arbeitsanweisungen für die Systemverwaltung der IT- und Kommunikationssysteme?	❑	❑
▪ Gibt es schriftlich festgelegte Verfahren, nach denen Sicherheitsvorfälle behandelt werden müssen?	❑	❑
▪ Werden Sicherheitsvorfälle systematisch analysiert/ dokumentiert?	❑	❑
▪ Gibt es schriftlich festgelegte Regeln für die Erstellung von Sicherheitskopien geschäftswichtiger Datenbestände?	❑	❑

- Gibt es kontinuierlich überprüfte Regeln, nach denen der Informationsaustausch mit Dritten vorgenommen wird? ❑ ❑
- Gibt es schriftlich fixierte Anforderungen an die Kontrolle des Zugangs zu Geschäftsinformationen? ❑ ❑
- Gibt es ein formales Anmelde- und Abmeldeverfahren für Benutzer von IT- und Kommunikationssystemen? ❑ ❑
- Wird eine Beschränkung des Zugriffs auf Informationen von den Systemen vorgenommen? ❑ ❑
- Werden elektronisch übermittelte Daten bezüglich ihrer Herkunft automatisch geprüft? ❑ ❑
- Werden Ereignisse identifiziert, die den kontinuierlichen Geschäftsbetrieb stören können? ❑ ❑
- Ist die Geschäftsführung/der Vorstand umfassend über alle Haftungsrisiken im Hinblick auf IT-Sicherheit informiert? ❑ ❑

Eigene Bemerkungen: _____

_____

_____

_____