macmon®

nac intelligent einfach

WARUM IT-SICHERHEIT OHNE NAC SCHEITERT

MACMON SECURE GMBH

macmon
nac intelligent einfach

Best of Breed NAC-Anbieter

- BSI-zertifizierte NAC-Lösung
- Erfahrenes Team mit Entwicklung, Support und Beratung an zentraler Stelle in Berlin
- Entwicklung von Sicherheitstechnologien und -standards
- Kooperation mit Forschungsinstituten und Hochschulen
- Erfahrung aus der Umsetzung von NAC-Projekten mit verschiedensten Branchen und unterschiedlichsten Netzwerkgrößen
- Kooperationen mit weiteren führenden Herstellern von Sicherheitstechnologien
- Mitglied der TRUSTED COMPUTING GROUP

NETWORK ACCESS CONTROL - NAC

macmon
nac intelligent einfach

„Wenn Sie Ihr Netzwerk wirklich schützen wollen, müssen Sie es kennen, inklusive aller Geräte und Technologien darin. (…). Der "subtile Unterschied" sei jener zwischen dem, was nach Ansicht eines Admins in seinem Netzwerk laufen sollte, und dem, was wirklich darin läuft.“

* Rob Joyce, Leiter TAO / NSA

NETWORK ACCESS CONTROL - NAC

macmon
nac intelligent einfach

Sie wissen bereits, was NAC bedeutet

Network Access Control:

- ✓ Gerätekontrolle – welches Gerät? → **NAC**
- ✓ Sicherheitsstatus prüfen → **COMPLIANCE**

→ Prüfen Sie die angebotene Lösung – was erhalten Sie wirklich?

NETWORK ACCESS CONTROL - NAC

macmon
nac intelligent einfach

Warum sollten Sie NAC einsetzen?

- Bundesdatenschutzgesetz (BDSG)
- Sarbanes-Oxley Act
- EuroSox (EU Directive No. 8)
- Basel II
- KonTraG
- MaRisk
- DIN EN 80001-1

BSI IT- GRUNDSCHUTZ-KATALOGE
Genehmigungsverfahren für IT-Komponenten

(Maßnahme 2.216):

„Die Installation und Benutzung nicht freigegebener IT-Komponenten muss verboten und die Einhaltung dieses Verbotes regelmäßig kontrolliert werden.“

ISO IT Sicherheitsstandard gemäß IEC 27001/17799

11.4.3 Equipment identification in networks „Automatic equipment identification should be considered as a means to authenticate connections from specific locations and Equipment“

ISO International Organization for Standardization

NETWORK ACCESS CONTROL - NAC

macmon
nac intelligent einfach

Die Bedeutung von NAC in der Praxis

Haben Sie jederzeit einen aktuellen Überblick über Ihr gesamtes Netzwerk?

Wissen Sie welche Geräte sich momentan in Ihrem Netzwerk befinden?

Werden Ihre Geräte stets überwacht und vor unbefugten Zugriffen geschützt?

Können Gast- und Mitarbeitergeräte sicher in Ihr Netzwerk integriert werden?

GESETZLICHE GRUNDLAGE

macmon
nac intelligent einfach

Die Änderung des „BSI-Gesetzes“:

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
IT-Sicherheitsgesetz vom 17. Juli 2015

§8a Sicherheit in der Informationstechnik kritischer Infrastrukturen

1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene **organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen**, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden.

§109a Daten- und Informationssicherheit

Nach Absatz 3 wird folgender Absatz 4 eingefügt:
(4) Werden dem Dienstanbieter nach Absatz 1 Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, **mit denen sie diese Störungen erkennen und beseitigen können.**

GESETZLICHE GRUNDLAGE

macmon
nac intelligent einfach

… und es kostet auch etwas

§14 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft, 2. einer vollziehbaren Anordnung nach § 8a Absatz 3 Satz 4 …zuwiderhandelt…

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 2 Buchstabe b mit einer Geldbuße bis zu hunderttausend Euro, in den übrigen Fällen des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

ANGRIFFE, DIE SO NICHT PASSIERT WÄREN…

macmon
nac intelligent einfach

- Es betrifft uns alle

Abo | Shop | E-Paper | Apps | Audio | Archiv | Spiele Jobs | Partnersuche | Immobilien | Automarkt

ZEIT ONLINE | DATENSCHUTZ

START POLITIK WIRTSCHAFT GESELLSCHAFT KULTUR WISSEN DIGITAL STUDIUM KARRIERE LE

Start › DIE ZEIT Archiv › Jahrgang: 2014 › Ausgabe: 16 › Wie ein Hacker ein Stadtwerk angreift

IT-SICHERHEIT

Blackout

Ein Hacker brauchte nur zwei Tage, um die Kontrolle über die Stadtwerke in Ettlingen zu übernehmen. Er zeigte: Die Stromnetze in Deutschland sind nicht sicher. VON CHRISTIANE GREFE

DIE ZEIT N° 16/2014 17. April 2014 08:37 Uhr | 31 Kommentare |

Abo | Shop | E-Paper | Apps | Audio | Archiv | Spiele Jobs | Partnersuche | Immobilien | Automarkt

ZEIT ONLINE | INTERNET

START POLITIK WIRTSCHAFT GESELLSCHAFT KULTUR WISSEN DIGITAL STUDIUM KARRIERE RE

Start › Digital › Internet › IT-Sicherheit: Auch Medizintechnik lässt sich hacken

IT-SICHERHEIT

Auch Medizintechnik lässt sich hacken

Überdosis nicht mehr ausgeschlossen: Der Sicherheitsforscher Billy Rios kann eine in Krankenhäusern verwendete Infusionspumpe über das Intranet manipulieren. VON JOHANNES WENDT

10. April 2015 17:15 Uhr 21 Kommentare |

Im Operationssaal des Universitätsklinikum Frankfurt | © Cathrin Müller/dpa

SPIONAGEAKTIVITÄTEN, DIE SO NICHT PASSIERT WÄREN…

macmon
nac intelligent einfach

- Schon fast amüsant:

Getauschte Drucker

- „angeblicher“ Servicepartner
- Drucker mit Festplatte getauscht
- Abzüge von allem, was gedruckt wurde

ÜBER MACMON ALS NEUE „MAC“
ERSICHTLICH UND GEBLOCKT

„BYOD“: ZWEI VERSCHIEDENE AUFFASSUNGEN

macmon
nac intelligent einfach

Behandlung von Smartphones und anderen Mobile Devices

MITARBEITEREIGENTUM

- Kein Zugriff
- Zugang gewähren
- Schutz des Netzwerks
- Anbieten bestimmter Ressourcen
  - Vorstandsvorgabe

FIRMENEIGENTUM

- Konfiguration des Devices
- Kontrolle der Daten
- Admin-Zugriff
- Remote Wipe
  - Vorstandsvorgabe

NETWORK ACCESS CONTROL „NAC“
+ BYOD PORTAL ZUR REGISTRIERUNG

MOBILE DEVICE MANAGEMENT
„MDM“

NETWORK ACCESS CONTROL - NAC

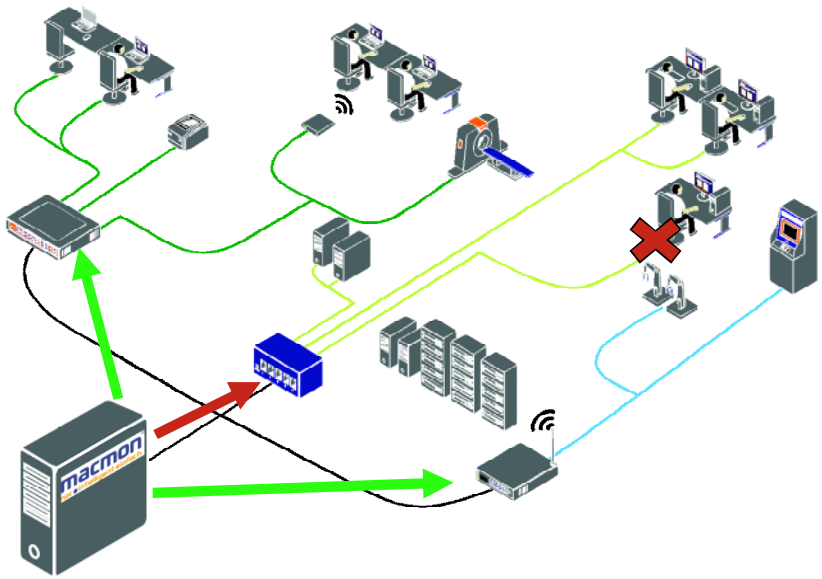
macmon
nac intelligent einfach

Warum also wird NAC so wenig genutzt?

- aufwändige Veränderungen der Infrastruktur?
- hohe Investitionskosten?
- hoher Pflegeaufwand?
- geringer bzw. schwer festzustellender Mehrwert?
- komplexe Thematik – hoher Schulungsaufwand?
- Gefahr, falsche bzw. zugelassene Systeme auszusperren?

ÜBERSICHT, KOMFORT & SICHERHEIT FÜR IHR GESAMTES NETZWERK

macmon
nac intelligent einfach



- Keine Agenten oder Sensoren erforderlich
- Keine Veränderungen der Netzwerkstruktur
- Herstellerunabhängigkeit
- Mischbetrieb mit & ohne 802.1X
- Angriffsabwehr & Netzwerktransparenz
- Lückenlose Übersicht aller Geräte

Gerätelokalisierung und -steuerung am Switch-Port – (SNMP, Telnet/SSH oder 802.1X)

MACMON ADVANCED SECURITY NEXT LEVEL

macmon
nac intelligent einfach

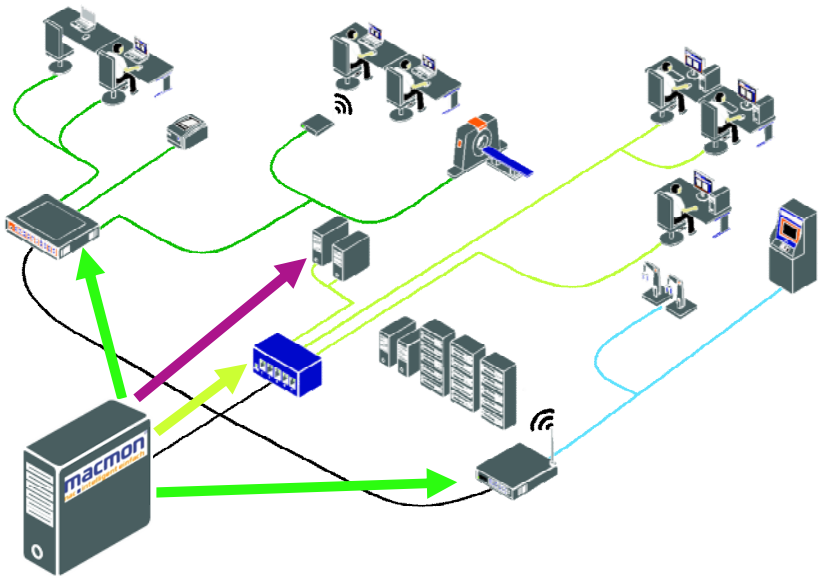
Das extra Level an Netzwerksicherheit

ERWEITERTE IDENTIFIZIERUNG DER ENDGERÄTE

- Reverse Authentication
- WMI & SNMP Corporate Check
- Footprinting

SCHUTZ VOR ANGRIFFEN

- Adressfälschung
- Angriffe auf Switches
- ARP-Spoofing/MAC-Spoofing

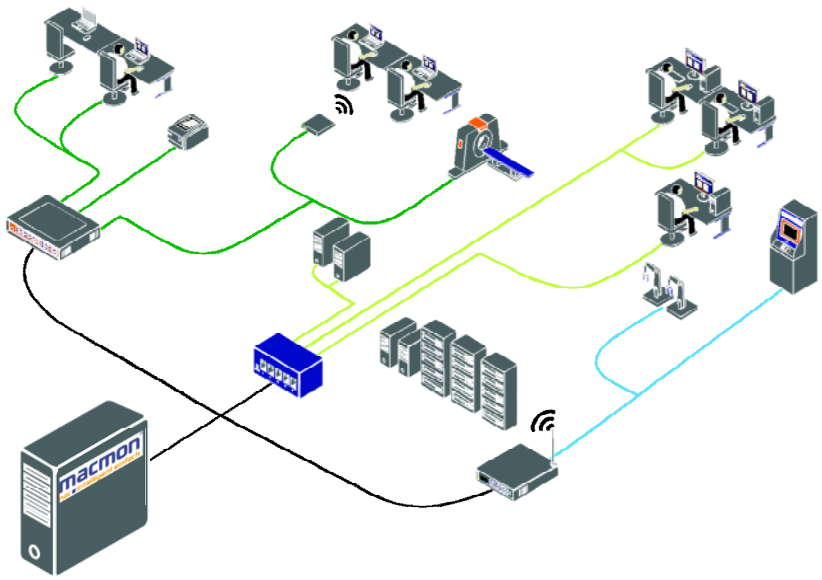


SNMP *IP-Adressauflösung über ARP* *Netzwerkdienste DNS und DHCP*

MACMON VLAN MANAGER

macmon
nac intelligent einfach

Statische und dynamische VLAN-Konzepte



Das VLAN wird durch das Endgerät bestimmt (MAC-Adresse › VLAN-ID).

Die Anwender haben immer den richtigen Zugang zum Netz, unabhängig vom physischen Anschluss.

- Einfache Pflege, keine Nachkonfigurationen bei Umzügen oder mobilen Nutzern.
- Kein Switch-Knowhow bei den für die Pflege eingesetzten Mitarbeitern notwendig.

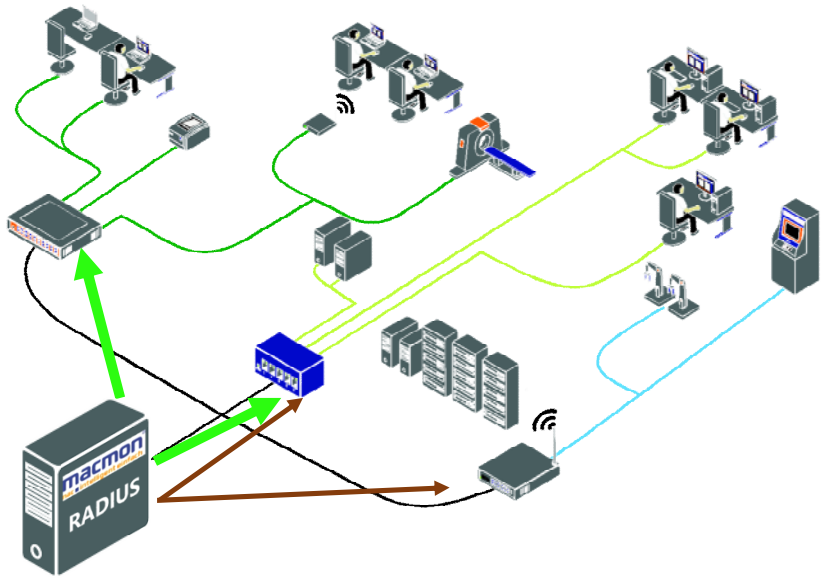
Gäste VLAN *Office-VLAN* *Produktions-VLAN*

MACMON IEEE 802.1X

macmon
nac intelligent einfach

Mischbetrieb mit & ohne 802.1X

- Switch führt Autorisierung über Radius-Protokoll durch.
  - MAB (MAC Authentication Bypass)
  - Identität & Passwort auch AD-Konten
  - Zertifikat
- Etablierung von Sicherheitszonen
- Die VLAN-Steuerung erfolgt über macmon



SNMP *EAP/802.1X*

MACMON IEEE 802.1X

macmon
nac intelligent einfach

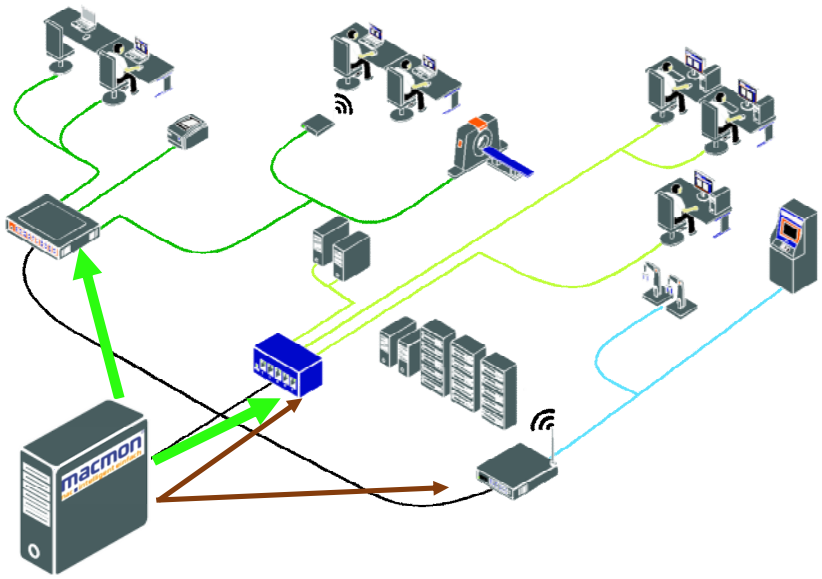
Ein Kinderspiel

- ✓ Intelligent einfache Anbindung von AD/LDAP und anderen Identitätsquellen mit „Mapping“
- ✓ Im gemischt betriebenen Einsatz – mit und ohne 802.1X
- ✓ Kombination von MAB mit macmon „Advanced Security Checks“
- ✓ Konfiguration von Gruppen ergibt automatische Regeln
- ✓ Intuitives und dynamisches Regelwerk
- ✓ Erleichterte Administration durch Gerätefokus
- ✓ Automatisiertes „Lernen“ von Geräten

MACMON NAC - IMPLEMENTIERUNG

macmon
nac intelligent einfach

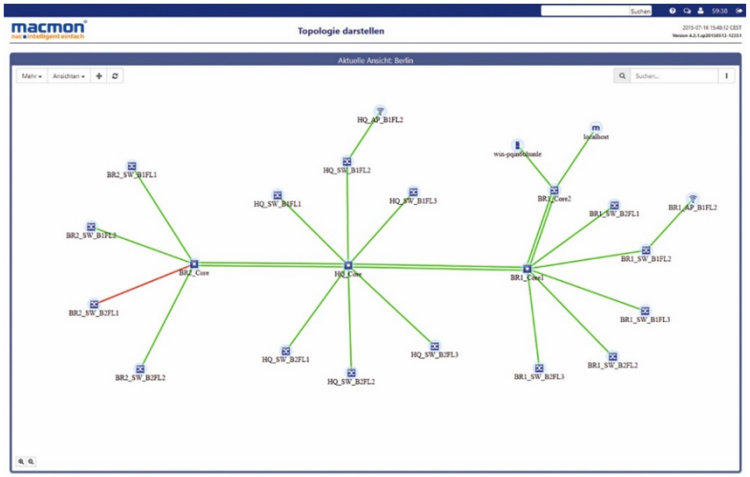
Innerhalb eines Tages, ohne Veränderung Ihrer Infrastruktur



- Erstellen einer Referenzliste
- Anbinden des Active Directorys und Lernen der Geräte (802.1X)
- Kommunikation mit allen Switchen
- Nur noch bekannte Geräte im LAN
- Unbekannte Geräte sperren/Gäste-LAN
- Eigene Geräte ins hinterlegte VLAN
- Einfache GUI – Intelligenz im Hintergrund
- Zeiteinsparungen durch Automatismen
- Angriffsabwehr & Netzwerktransparenz

MACMON GRAFISCHE TOPOLOGIE

Komfortable und automatische Visualisierung

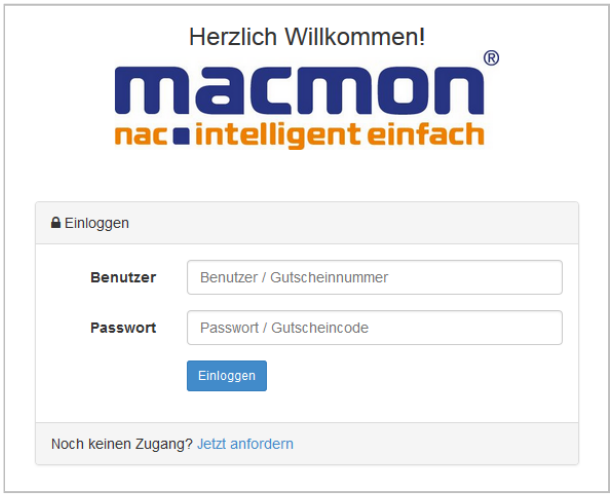


macmon hat im Betrieb automatisch alle Informationen:

- Automatisches Anordnen und Ergänzen von neuen Endgeräten.
- Filtern anhand von Eigenschaften wie IP-Adresse, Name, VLAN, etc.
- Speichern, Laden und Exportieren als .SVG
- Fehlkonfigurationen finden und manuell Uplinks pflegen

MACMON GUEST SERVICE

Intelligente Kontrolle aller nicht-Unternehmensgeräte



- ✓ Individuelle Gestaltung des Captive-Portals
- ✓ Nutzung verteilter Instanzen mit unterschiedlichem Layout
- ✓ Unabhängig vom Hersteller der LAN/WLAN-Infrastruktur
- ✓ Ortung der Geräte (an welchem Access-Point)
- ✓ Reaktives Aussperren der Geräte
- ✓ Selbstregistrierung mit Handy-Nr. und User-Namen
- ✓ Erstellung von Voucher-Listen zur Vereinfachung des Ablaufs am Empfang
- ✓ Sponsor Portal & BYOD-Portal
- ✓ AD/LDAP Integration

MACMON COMPLIANCE

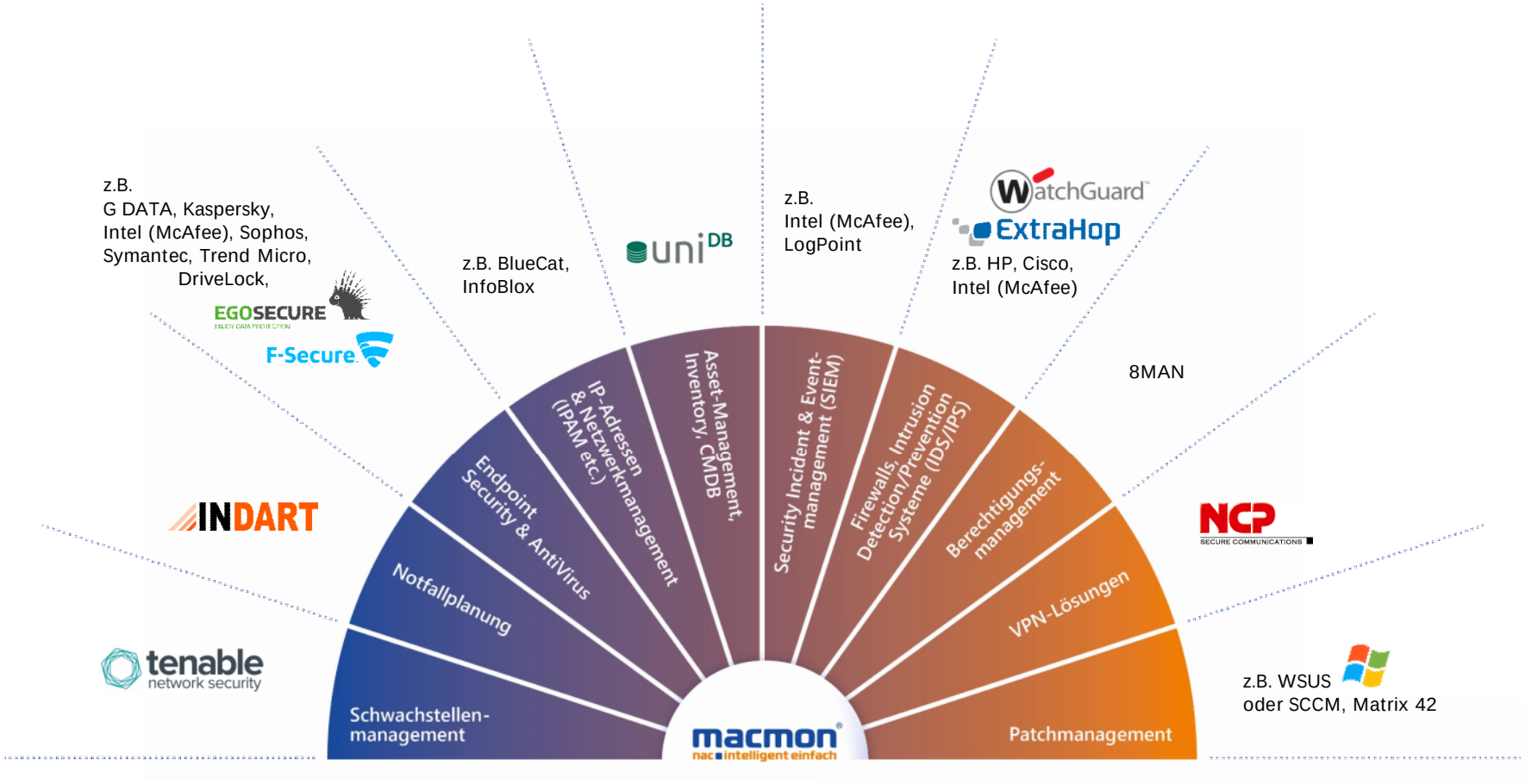
macmon
nac intelligent einfach

Automatische Reaktion auf Sicherheitsverstöße

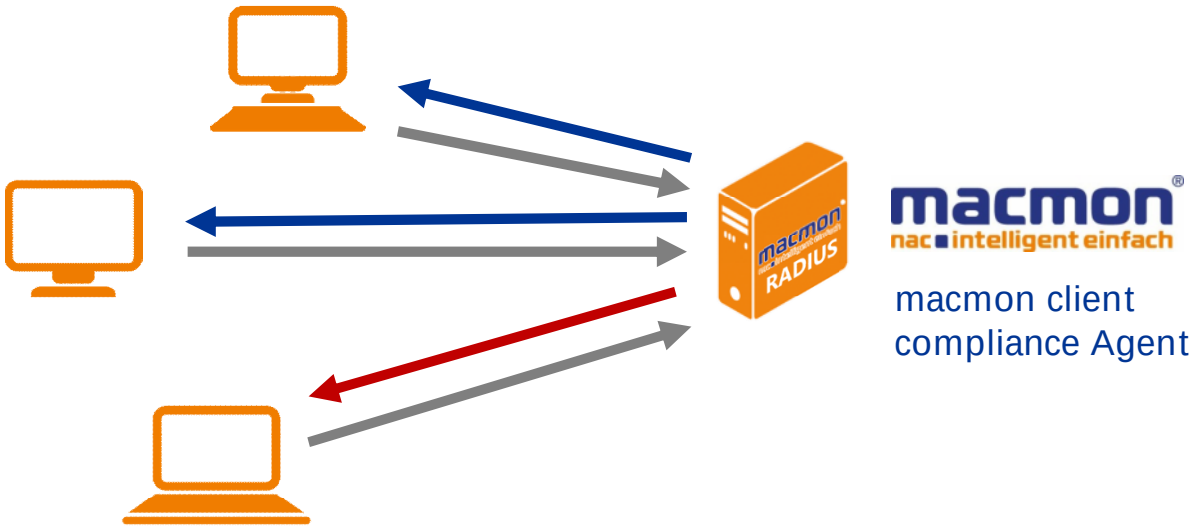
- multiple Compliance – Umsetzung der Vorgaben verschiedener Systeme gleichzeitig durch Nutzung der offenen Schnittstelle
- antivirus connector – Anbindung führender Anti-Virus-Systeme
- Aktive Statusänderung durch den macmon-eigenen Compliance Agenten
- Integrierte IF-MAP Technologie

➡ Sofortige Erhöhung des ROI durch Nutzung aller vorhandenen Systeme

MACMON NAC – TECHNOLOGIEPARTNER/KOPPLUNGEN



MACMON CLIENT COMPLIANCE



Scan Daten *compliant* *non-compliant*

MACMON ENERGY

Energieverbrauch reduzieren & Produktivität verbessern

macmon tauscht die Energieprofile & weckt die PC's über WakeOnLan

Zeitgesteuert: z. B. werktags um 18:00 Uhr/8:00 Uhr

Ereignisgesteuert durch die Zutrittskontrolle

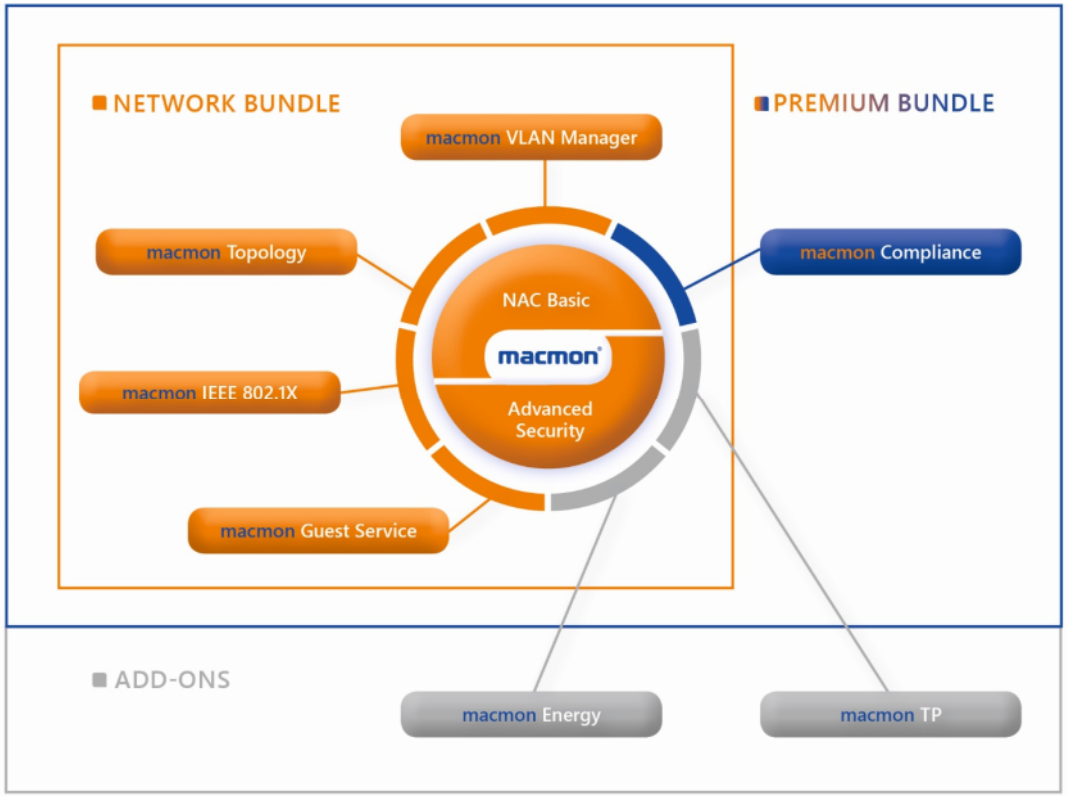
Geplant durch den Anwender mit dem macmon energy-Kalender:
Urlaube, Abwesenheit etc. können hinterlegt werden

Zur Vermeidung von Risikosituation wie:
Angriffe, Verbreitung von Viren, Ausnutzen als Bot

Zur Ausführung von automatisierten Wartungs- und
Supportarbeiten wie: Software-Updates, vollständige Virenscans, Backups

MACMON PRODUKTFAMILIE

Abgestimmte Sicherheitspakete



KUNDEN ÜBER DIE VORTEILE VON MACMON NAC

macmon
nac intelligent einfach

- ✓ Sofortige Netzwerkübersicht mit grafischen Reports & Topologie
- ✓ Einführung innerhalb eines Tages & intuitives tägliches Handling
- ✓ Mischbetrieb mit und ohne 802.1X
- ✓ Intelligente AD Integration mit dynamischem Regelwerk
- ✓ Hoch flexibles „Gäste“-Portal
- ✓ Sinnvolle Integrationen mit anderen Security-Produkten
- ✓ Herstellerunabhängigkeit
- ✓ BSI-zertifizierte NAC-Lösung
- ✓ Deutscher Hersteller-Support

DIESE KUNDEN SETZEN MACMON NAC EIN

macmon
nac intelligent einfach

Das Auto.
miRO
playmobil
VORWEG GEHEN
MBDA MISSILE SYSTEMS
HARTING
SWR
NRW radio NRW
arvato MOHN MEDIA
FASSMER
BSR
RAG
THE LINDE GROUP Linde
Zentrum für Informationsverarbeitung und Informationstechnik
Baden Baden
LWVHessen
LBA
STADT ESSLINGEN AM NECKAR
Landratsamt Sigmaringen
SACHSEN Landesamt für Steuern und Finanzen
kfw BANKENGRUPPE
Investitionsbank Berlin
Sparkasse Arnstadt-Ilmenau
Volksbank Odenwald
universa VERSICHERUNGEN
JOSEPHS-HOSPITAL WARENDORF
Klinikum Braunschweig
Paulinenpflege Winnenden
Universitätsklinikum Carl Gustav Carus DIE DRESDNER.
isas
HZB Helmholtz Zentrum Berlin

KUNDENBEISPIELE – INDUSTRIE

macmon
nac intelligent einfach

Wichtige Faktoren

Roboter und Maschinen können nicht mit üblichen Mitteln (Virenschutz, Patches, …) geschützt werden

Dienstleister müssen für Störungsbeseitigungen und Wartungsarbeiten Zugang zum Netz haben

Sicherheitsvorfälle können Sach- und Personenschäden bewirken

Produktionsnetze „wachsen“ oft unkontrolliert, da proprietäre Kommunikationssysteme (Feldbus, Interbus, Profibus, …) zunehmend durch Ethernet ersetzt werden

KUNDENBEISPIELE – GESUNDHEITSWESEN

macmon
nac intelligent einfach

Wichtige Faktoren

Handbuch – Umsetzung DIN EN 80001-1 mit macmon NAC verfügbar!

medizinisches IT-Netzwerk und allgemeines IT-Netzwerk müssen getrennt werden (DIN EN 80001-1, Risikomanagement für IT-Netzwerke mit Medizinprodukten)

Schutz der Arzt-Patientenbeziehung bzw. Wahrung des Patientengeheimnisses (ärztl. Schweigepflicht, § 203 StGB)

für private Träger: Beim Rating von Basel II (künftig auch EURO-SOX), ist die IT-Infrastruktur direkt an die Erteilung von Finanzmitteln durch Banken gekoppelt; Defizite in der IT-Sicherheit führen i.d.R. zur Kürzung der Kreditlinie

JOSEPHS-HOSPITAL WARENDORF

Klinikum Braunschweig

Universitätsklinikum Carl Gustav Carus DIE DRESDNER.

Paulinenpflege Winnenden

das IT-Netzwerk wird durch die Einbindung von Medizinprodukten zu einem medizinischen IT-Netzwerk und fällt somit in den Zuständigkeitsbereich des Medizinproduktegesetzes (MPG)

KUNDENBEISPIELE – BANKEN & VERSICHERUNGEN

macmon
nac intelligent einfach

Wichtige Faktoren

kfw BANKENGRUPPE | Investitionsbank Berlin | Sparkasse Arnstadt-Ilmenau | universa VERSICHERUNGEN | Volksbank Odenwald

Geldautomaten und andere NAC-GAP Geräte im Netz sind in die Sicherungsmaßnahmen einzubeziehen

Sicherung öffentlicher Bereiche mit Publikumszugang ist erforderlich

die ausgeprägte Filialstruktur kann durch eine Live-Überwachung effektiv kontrolliert werden

MaRisk ist ab 1. Januar 2008 bindend (Umsetzung durch Anwendung von BSI- und ISO-Normen – hoher Sicherheitsanspruch)

KUNDENBEISPIELE – WISSENSCHAFT & FORSCHUNG

macmon
nac intelligent einfach

Wichtige Faktoren

Innovationen deutscher Forschungs- und Entwicklungseinrichtungen sind begehrtes Ziel von wissenschaftlicher und wirtschaftlicher Konkurrenz

Sicherheitsvorfälle können Abfluss von Know-How und Forschungsdaten bewirken, und damit mittelbar auch die Wettbewerbsfähigkeit gefährden

Gaststudenten/Gastwissenschaftler, Gäste und externe Mitarbeiter bedürfen abgestufter Zugangs- und Zugriffsberechtigungen

Die Live-Überwachung erleichtert die Kontrolle und Steuerung in weit gefächerten Organisationsstrukturen, auch weltweit

macmon ermöglicht die Administration mit wenig Personalkapazität

isgs

HZB Helmholtz Zentrum Berlin

KUNDENBEISPIELE – BEHÖRDEN

macmon
nac intelligent einfach

Wichtige Faktoren

Zentrum für Informationsverarbeitung und Informationstechnik

Baden Baden

LWVHessen

LBA

STADT ESSLINGEN AM NECKAR

Landratsamt Sigmaringen

SACHSEN
Landesamt für Steuern und Finanzen

klare Anforderungen des BSI sind zu erfüllen

macmon ermöglicht die Administration mit wenig Personalkapazität

die Live-Überwachung erleichtert die Kontrolle und Steuerung in weit gefächerten Organisationsstrukturen, auch weltweit

Bundesamt für Sicherheit in der Informationstechnik
Deutsches IT-Sicherheitszertifikat
Zertifikat Nummer:
BSI-DSZ-CC-0738-2015
Gültig bis: 08.11.2020
bis EAL 4

aus der Verarbeitung sensibler, oft personenbezogener Daten resultiert ein besonders hoher Schutzbedarf

KUNDENBEISPIELE – MEDIEN

macmon
nac intelligent einfach

Wichtige Faktoren

viele mobile Arbeitsplätze, die oft außerhalb oder sogar im Ausland eingesetzt werden

viele Gäste und externe Mitarbeiter auf dem Firmengelände

die Live-Überwachung erleichtert die Kontrolle und Steuerung in weit gefächerten Organisationsstrukturen, auch weltweit

macmon ermöglicht die Administration mit wenig Personalkapazität

SWR

NRW radio NRW

arvato MOHN MEDIA

KONTAKT

- Wir freuen uns auf das persönliche Gespräch mit Ihnen!

macmon secure GmbH

Alte Jakobstraße 79-80
10179 Berlin

T: +49 30 23257770
F: +49 30 2325777-200

E: vertrieb@macmon.eu
www.macmon.eu