CYBER SECURITY

Threat Protection
Network Security | Endpoint Security | Encryption | Credential Management | Awareness | E-Mail Security

Incident Response
Endpoint Detection & Response | Health Checks | Computer Emergency Response Team | Security Operation Center

IT Penetration Tests
OSINT | Blackbox Penetrationtest | ISM/Wifi Spektrumanalyse | Webapplikation Pentest | Social Engineering Attack

persönlich. /// kompetent. /// ein Team.

1994
gegründet

über
490
Mitarbeiter

185,5
Millionen
Umsatz
2019

7
Standorte

WILLKOMMEN BEI IHREM IT PARTNER!

IT FÜR SIE!

Unsere langjährige Zusammenarbeit mit Kunden soll uns auch weiterhin ein Ansporn sein, mit unserem Lösungsportfolio zu überzeugen:

MR Datentechnik ist Fullservice-Dienstleister und bietet Ihnen ein besonders breites Portfolio aufeinander abgestimmter IT Leistungen.

Die Bereiche IT Services, IT Solutions und Managed Services sind eng miteinander verzahnt. Profitieren Sie von engagierten Ansprechpartnern und kurzen Reaktionszeiten. Unsere Kompetenzteams agieren professionell und flexibel.

Wir sind in Ihrer Nähe: Der Hauptsitz von MR Datentechnik befindet sich in Nürnberg und wird von Niederlassungen in Bamberg, Bayreuth, Melle, München, Regensburg und Würzburg unterstützt. Mit unseren bundesweiten Partnern sind wir immer in Ihrer Nähe.

LÖSUNGEN
IM ÜBERBLICK

ESSENTIELL

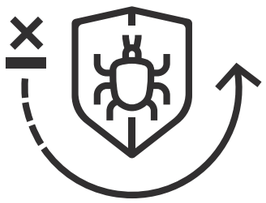
THREAT PROTECTION

Seite 6 – 9

- Network Security
- Endpoint Security
- Encryption
- Credential Management
- Awareness
- E-Mail Security

AKUT

INCIDENT RESPONSE

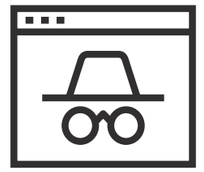


Seite 10 – 11

- Endpoint Detection & Response
- Health Checks
- Computer Emergency Response Team
- Security Operation Center

PRÄVENTIV

PENETRATIONS TESTS



Seite 12 – 14

- OSINT
- Blackbox Penetrationstest
- ISM/Wifi Spektrumanalyse
- Webapplikation Pentest
- Social Engineering Attack

IHR PARTNER

IHRE VORTEILE

Steigerung der IT-Sicherheit

Aktuellste Konzepte & Lösungen

Modulare & Flexible Lösungen

Betreuung im aktiven Betrieb

WIR SCHÜTZEN SIE VOR ANGRIFFEN!

THREAT PROTECTION

#NextGenFirewall
NETWORK SECURITY

Netzwerkinfrastrukturen schützen und verbessern. Von einer Perimeter-Firewall zu einer Lösung zur Optimierung verteilter Netzwerke, die über eine beliebige Anzahl von Standorten und Applikationen skalierbar ist, lokale und Cloud-Infrastrukturen verbindet und Unternehmen bei der Transformation ihres Geschäftsmodells unterstützt. Darüber hinaus mit intelligentem Traffic-Management und WAN-Komprimierung. Das interne Netzwerk vor unerwünschten Geräten oder Eindringen schützen und eine aktuelle Übersicht von Netzwerkgeräten beschaffen.

#DataProtection
ENCRYPTION

Daten überall ganz automatisch schützen. Zentral verwaltete Festplattenverschlüsselung und die betriebssystemeigenen Verschlüsselungstechnologien Windows BitLocker und Mac FileVault nutzen. Verwalten Sie Schlüssel und Wiederherstellungsfunktionen nahtlos über ein Management Center. Um Ihren Workflow weiter zu vereinfachen, können Sie Windows- und macOS-Festplattenverschlüsselungen nun zentral verwalten. Verschlüsseln von einzelnen Daten, diese bleiben auch dann verschlüsselt, wenn diese sich in Netzlaufwerken, auf USB-Devices oder in die Cloud übertragen werden.

#AntiRansomware
ENDPOINT SECURITY

Im Zuge der Digitalisierung Ihrer Betriebsabläufe müssen Sie sämtliche Server, Laptops und mobilen Geräte schützen. Wir bieten Next-Generation-Sicherheit in einer einzigen Lösung, mit der Sie jeden Endpoint in Ihrem Unternehmen gegen Cyber-Angriffe schützen können.

#Blacklists
E-MAIL SECURITY

Mit der MR Mailsecurity stellen wir entweder einen Shared, bzw. auf Wunsch auch dedizierten Dienst bereit, der wichtige Aufgaben im Bereich der Mailkommunikation erledigt. Die Lösung stellt unter anderem sicher, dass sowohl eingehende als auch ausgehende E-Mails mit Schutzmechanismen wie Malwareprüfung, Sandboxing, Spamprüfung, Data Loss Prevention gescannt werden und ggf. quarantänisiert oder verworfen werden. Die MR Mailsecurity Lösung gibt es sowohl als Full Managed Services als auch als dedizierte Lösung bei unseren Kunden, entweder virtuell oder als Hardwarebox. Ergänzt werden kann der Service durch eine umfassende E-Mail Archivierungslösung, ebenfalls als Service oder Appliance.

#PasswordManagement
CREDENTIALS MANAGEMENT

Schützen Sie Ihre Daten vor unbefugten Zugriffen durch Dritte. Eine zentralisierte Datenbank gewährleistet eine sichere Zusammenarbeit im Team. Freigaben werden zeitlich begrenzt vergeben sowie Zugriffe rollenbasiert kontrolliert. Der Abruf eines Passworts ist zu jedem Zeitpunkt nachweisbar. Die Eintragung von Passwörtern in Anmeldefeldern von Internetseiten, der Import von Benutzern und Strukturen aus dem Active Directory, sowie das Generieren neuer Passwörter oder das Managen privilegierter Accounts – alles läuft automatisiert.

#OnlineTrainingPlatform
AWARENESS

MR Bait
Don't get phished!

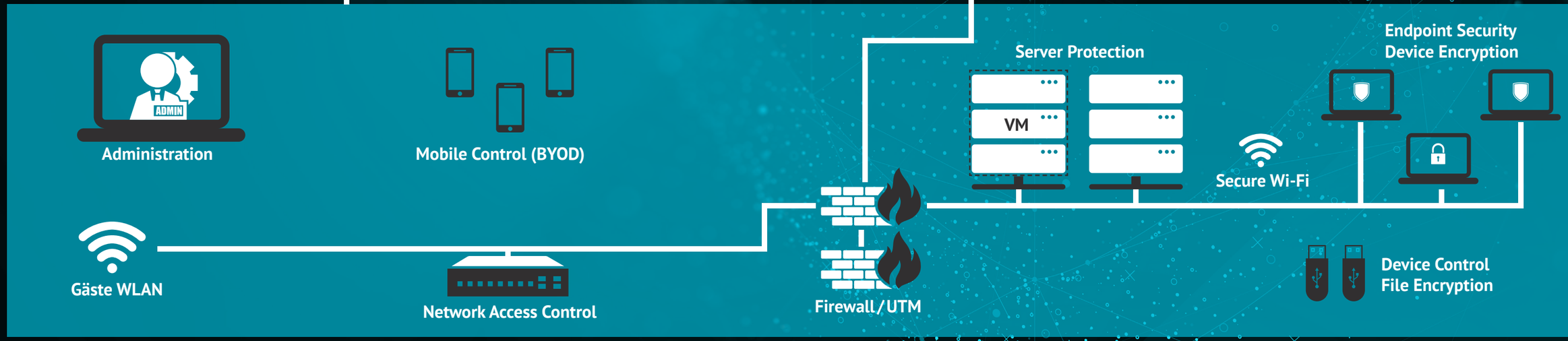
Eine große potenzielle Bedrohung der „Informationssicherheit“ besteht im Inneren des Unternehmens: bei den Beschäftigten. Meist werden aus Gutgläubigkeit, Neugierde oder Konfliktvermeidung sicherheitskritische Handlungen vorgenommen. Klar, denn das Thema Sicherheit ist für jeden IT-Mitarbeiter allgegenwärtig und durch die Medien nahezu täglich präsent. Aber können Sie mit Gewissheit sagen, wie verantwortungsbewusst Ihre Mitarbeiterinnen und Mitarbeiter tatsächlich mit diesen sensiblen Informationen umgehen?

SECURITY ENVIRONMENT

HOME OFFICE | ON THE MOVE

REMOTE OFFICE

ZENTRALE



WIR SIND FÜR SIE DA, AUCH IM NOTFALL!

INCIDENT RESPONSE

#ForensischeAnalysen

ENDPOINT DETECTION & RESPONSE

Mit Endpoint Detection & Response (EDR) können Unternehmen Ausmaß und Folgen von Sicherheitsvorfällen verstehen, Angriffe aufspüren, die eventuell noch nicht bemerkt wurden, Dateien analysieren und bestimmen, ob es sich um Bedrohungen handelt, und jederzeit zuverlässig Auskunft über ihren Sicherheitsstatus geben.

#Analyse

HEALTH CHECK

Gesundheitsvorsorge ist in aller Munde – doch sorgen Sie nicht nur für Ihre Gesundheit, sondern auch für die Sicherheit Ihres Unternehmens vor.

Der MR Security Health Check beinhaltet:

- Security Health Check vor Ort gemäß Checkliste durch unsere zertifizierten Spezialisten
- Geprüft werden Ihre Firewall, Endpoint Protection und Verschlüsselungslösung (Nur für Produkte von supporteten Herstellern)
- Überprüfung Ihrer Systemauslastung
- Kurze Dokumentation inkl. Bestandsaufnahme zum IST-Zustand und daraus ggf. resultierende Handlungsempfehlungen

#IncidentMonitoring

SECURITY OPERATION CENTER

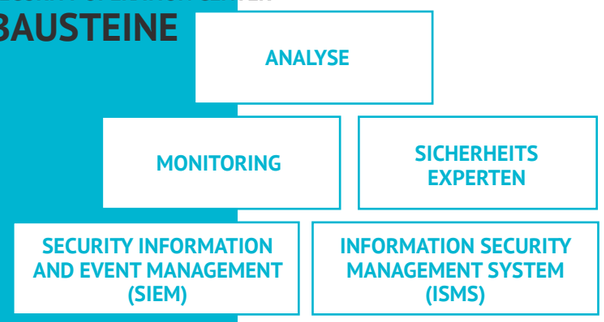
MR betreibt das Security Operation Center (SOC) in Ihrem Unternehmen und übernimmt den laufenden Betrieb als Managed Service. In kürzester Zeit operativ, nach bewährten Prinzipien und basierend auf modernster Technologie. Persönliche Ansprechpartner sind jederzeit direkt für Sie erreichbar.

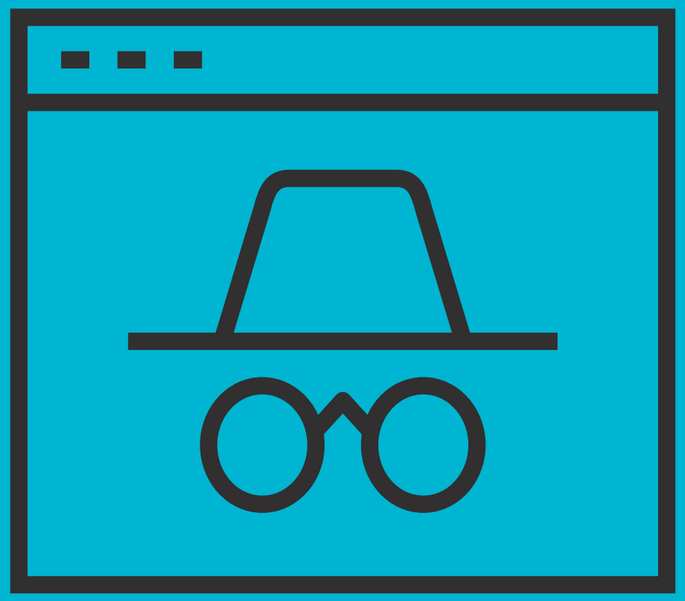
Klare Regelungen und dokumentierte Prozesse ermöglichen strukturierte Abläufe und einfache Kommunikation mit Ihrem Unternehmen. Wählen Sie die für Sie passenden Servicezeiten bis zu 24/7 aus. Incident Response und Echtzeit-Alarmierung inklusive.

- **Proaktive Überwachung der IT-Systeme und laufende Analysen zur aktuellen Bedrohungslage**
- **Erkennen von Schwachstellen der IT-Sicherheit und deren Beseitigung**
- **Zentrales Sicherheitsmanagement für die unterschiedlichen Devices/ Lösungen**
- **Alarmierung bei erkannten Angriffen und Bedrohungen**
- **Direkte Abwehrmaßnahmen zur Schadensbegrenzung von Cyber-Attacken**
- **Durchführung von Security-Assessments**

SECURITY OPERATION CENTER

BAUSTEINE





WIR HACKEN, UM SIE ZU SCHÜTZEN!

PENETRATIONS TESTS

#Hacker-Perspektive

INFORMATIONS-BESCHAFFUNG MIT OSINT

In diesem Schritt sammelt der Angreifer alle Informationen aus dem Clear-Web und dem Darknet, welche er zu dem jeweiligen Opfer findet, trägt diese zusammen, strukturiert diese und schafft sich somit ein komplettes Bild über das Unternehmen/die Privatperson, welche angegriffen wird. Dabei werden mitunter spezielle OSINT-Tools benutzt, die teilweise umfangreiche Recherchearbeiten automatisieren.

#Funkanalyse

ISM | WIFI SPEKTRUMANALYSE

Ermittlung und Katalogisierung aller vorhandenen Radio Devices in einem Unternehmen. Dabei wird ein Wireless Radio Device Abdruck auf physikalischer Ebene erstellt, um ggf. Eingaben mit einer Wireless-Tastatur abzufangen und gezielt zu manipulieren, um diese zu einem späteren Zeitpunkt zu wiederholen (Passworteingaben etc.).
Des Weiteren werden entsprechende WLAN-Schutzmechanismen, wie z.B. IEEE 802.1x geprüft und bewertet.

#powered by

whitelisthackers
[cyber attack investigation and research]

#Phishing

SOCIAL ENGINEERING ATTACK

In diesem Modul geht es weniger darum (anders als in den vorherigen Modulen), wie gut der Kunde seine IT technisch abgesichert hat, sondern wie gut die Mitarbeiter sensibilisiert sind. Mittels gezielter Angriffs¬methoden (Phishing-Emails, USB-Sticks am Parkplatz, Netz¬werkdosen IM und AM Gebäu¬de) wird versucht, Zugriff auf sensible Unternehmensdaten immer mithilfe des Mitarbei¬ters, welcher bei dem „Opfer-Unternehmen“ beschäftigt ist, zu bekommen. In diesem Modul sind nicht nur technische, sondern auch psychologische Skills gefragt, um das Vertrauen der Belegschaft zu gewinnen.

#SQL-Injection

WEBAPPLIKATIONEN PENETRATIONSTEST

In diesem Modul wird einerseits die Sicherheit des konfigurierten Webservers, sowie natürlich auch der gehosteten Applikation auf die Probe gestellt. Mittels unterschiedlicher Angriffsvektoren versucht der Angreifer hier Code in das System einzuschleusen, bzw. mittels SQL-Injections entsprechende Datenbankbefehle zu platzieren. Diese Angriffsmethode ist die erfolgreichste Methode, um Schwächen in der Infrastruktur des Unternehmens festzustellen.

#Einfachmaldraufloshacken

BLACKBOX PENETRATIONS-TEST

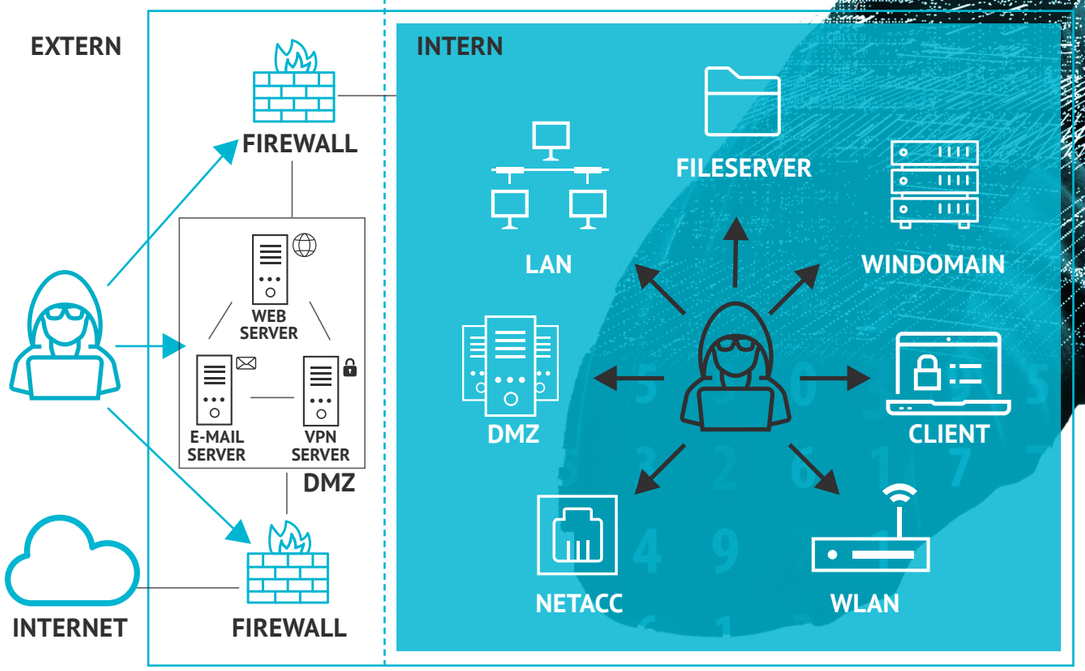
In diesem Schritt verwendet der Angreifer unter anderem die Informationen, die er im OSINT Teil gewonnen hat und startet einen Angriff auf die gefundenen Systeme nach dem Blackbox-Verfahren (wir wissen nicht, was das System tut, was es macht und was es kann). Dabei werden unterschiedliche Angriffsvektoren und Vulnerabilities ausgenutzt. Des Weiteren werden potenzielle Eingangstüren (z.B. VPN Gateways) dabei gezielt angegriffen.

PENETRATIONSTEST
WIE GEHEN WIR VOR?

Ein Penetrationstest ist im Wesentlichen die Simulation eines Angriffes auf ein definiertes Zielsystem. Dabei „simulieren“ unsere Analysten eine realistische Attacke eines typischen Angreifers. Im Gegensatz zu einem tatsächlichen Angriff wird dabei kein vorsätzlicher Schaden angerichtet. Wie bei einem realen Angriff versuchen wir Zugriff auf sensible Daten oder Systeme zu erhalten. In diesem Zusammenhang bedeutet risikoorientiert, dass wir die Erfolg versprechendsten Angriffsvektoren am gründlichsten überprüfen. Mit Hilfe eines Penetrationstests stellen wir das aktuelle Sicherheitsniveau fest, decken Schwachstellen auf, geben Handlungsempfehlungen zur Verbesserung der IT-Sicherheit und bewerten diese nach Aufwand und Dringlichkeit. So verbessern Sie den Schutz Ihrer IT-Systeme.

PENETRATIONSTEST
PHASE 1: EXTERN

PENETRATIONSTEST
PHASE 2: INTERN



UNSERE PARTNER

SOPHOS
Cybersecurity evolved.

Barracuda

kaspersky

macmon
nac intelligent einfach

SEPPMAIL

FORTINET

DUO

Mo-Fr | 07:00 Uhr – 17:00Uhr

CYBER SECURITY TEAM

+49 (0) 911 52147 564

security@mr-daten.de

MR | Bamberg
bamberg@mr-daten.de
+49 951 91767-0

MR | Bayreuth
bayreuth@mr-daten.de
+49 921 72651-0

MR | Melle
melle@mr-daten.de
+49 5422 92136-0

MR | München
muenchen@mr-daten.de
+49 89 4520944-0

MR | Regensburg
regensburg@mr-daten.de
+49 941 30764-0

MR | Nürnberg
info@mr-daten.de
+49 911 52147-0

MR | Würzburg
wuerzburg@mr-daten.de
+49 931 35960-0