



Fünf Möglichkeiten zum Schutz kritischer Infrastrukturen

Inhaltsverzeichnis

Kurzfassung	3
Definition „kritische Infrastrukturen“	3
Sicherheitsprobleme im Zusammenhang mit kritischen Infrastrukturen	4
Nicht auf Sicherheit ausgelegt	5
Das Problem ist real	5
Weltbank mindestens sechsmal bestohlen	6
Ehemaliger Mitarbeiter erst nach 46. Angriff gestoppt	6
Sicherheitsmaßnahmen für unnötig befunden	6
Zensur von politischen Protesten	6
Remote-Zugriff ausgenutzt	7
Viren dringen in kritische Netzwerke ein	7
Die Lösung: Fünf wesentliche Möglichkeiten zum Schutz kritischer Infrastrukturen	7
1. Ausbringung von Echtzeitschutz	7
Echtzeit-Angriffe erfordern Echtzeit-Schutz	8
2. Abtrennung und Abschirmung kritischer Infrastrukturen von verbundenen Netzwerken	8
Erste Schutzstufe: die Firewall	8
Zweite Schutzstufe: Intrusion Prevention	9
3. Kontrolle der Zugriffsberechtigungen und Netzwerkaktivitäten	10
4. Schutz von Daten über kritische Infrastrukturen vor Datendiebstahl	11
5. Ausbringung eines zuverlässigen Schutzes ohne Beeinträchtigung von Verfügbarkeits-,Integritäts- und Zuverlässigkeitsanforderungen	12
McAfee-Produkte und -Technologien für den Schutz kritischer Infrastrukturen	12
McAfee TrustedSource	12
McAfee Firewall Enterprise	13
Bevorzugte Wahl für kritische Infrastrukturen	14
McAfee Network IPS	15
McAfee UTM Firewall	15
McAfee Network Access Control Module	16
McAfee Network User Behavior Analysis	16
McAfee Network DLP Manager	16
McAfee Email Gateway	16
McAfee Web Gateway	16
Kombinierter Schutz	17
Zusammenfassung	17
Informationen zu McAfee	18

Kurzfassung

Bis vor kurzem war die „Sicherheit wichtiger Ressourcen“ oder der „Schutz wichtiger Infrastrukturen“ kein Thema. Die wichtigen Netzwerke und Systeme zur Steuerung der Strom-, Wasser-, Öl- und Gasversorgung sowie der ÖPNV-Netze waren genau wie Fertigungssysteme von der restlichen EDV-Welt getrennt. „Security by Obscurity“ war das Motto, und diese Trennung bedeutete, dass Verantwortliche für wichtige Ressourcen sich keine Sorgen über Internetangriffe machen mussten.

Der Aufstieg des Internets und die schnelle Verbreitung kostengünstiger Breitbandanschlüsse jedoch haben wichtige Systeme in Gefahr gebracht. Die überwältigende Mehrheit dieser Systeme ist mittlerweile mit IT-Systemen verbunden und wird von Anwendern per Remote-Zugriff über drahtlose Geräte bedient sowie von nicht vertrauenswürdigen Personen genutzt, um Data Mining-Möglichkeiten für ihre Unternehmen zu bieten. Auch werden die Systeme in die Netze unabhängiger Systembetreiber und anderer Drittparteien eingebunden, um eine übergreifende Koordination mehrerer Unternehmen zu ermöglichen.

Somit können Sicherheitsbedrohungen, die seit Jahrzehnten ständige Begleiter von IT-Systemen sind, sich nun auch praktisch unentdeckt auf kritische Infrastruktursysteme ausbreiten und diese Systeme anfällig gegenüber Hackern, Saboteuren und Computerkriminellen in aller Welt machen.

Dieses Dokument stellt fünf wesentliche Möglichkeiten zum Schutz der kritischen virtuellen Infrastrukturen der Welt dar und informiert über aktuelle Bedrohungen und Schwachstellen.

Definition „kritische Infrastrukturen“

Kritische Infrastrukturen sind sämtliche Computersysteme in den Netzwerken der Energiewirtschaft, die ein Ziel für Vireneinfektionen, Denial-of-Service-Angriffe, terroristische Anschläge, Spionage und Sabotage darstellen könnten. Im schlimmsten Fall könnten Angriffe auf diese Netzwerke zu Todesfällen führen, die Sicherheit der Öffentlichkeit bedrohen, die nationale Sicherheit gefährden, umfassende wirtschaftliche Umwälzungen provozieren oder Umweltkatastrophen verursachen. Bedrohte Systeme sind in den folgenden Bereichen zu finden:

- *Energiewirtschaft* – Stromübertragungs- und Vertriebsnetze, Öl- und Gaspipelines, Wasserverteilung und -versorgung sowie radioaktive Stoffe und Kernkraftwerke
- *Transportwesen* – Straßen-, Schienen- und Lufttransport, ÖPNV-Netze, Logistik und Gefahrguttransporte
- *Staatliche und kommunale Dienste* – Wassersysteme und Müllentsorgung
- *Prozessfertigung* – Chemische und petrochemische Abfälle und Sondermüll
- *Informations- und Kommunikationstechnik* – Telekommunikation, Fernsehen und Radio
- *Notdienste* – Rettungsdienste, Gesundheitswesen, Feuerwehr und Polizei
- *Bank- und Finanzwesen* – Handelssysteme, Netzwerke für automatische Verrechnung und Geldautomatennetze

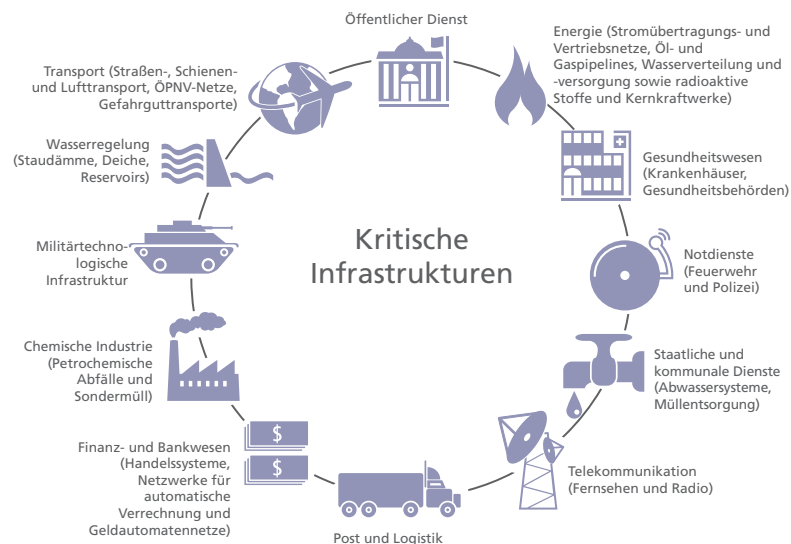


Abbildung 1: Branchen, in denen kritische Infrastrukturnetze betrieben und verwaltet werden.

Die Zerstörungen durch eine einzige Welle Computerangriffe auf kritische Infrastrukturen in den USA könnten Schäden von über 700 Milliarden US-Dollar verursachen – das wäre so viel wie 50 schwere Hurricanes, die gleichzeitig über das Land hereinbrechen.

(Quelle: U.S. Cyber Consequences Unit, Juli 2007)

Sicherheitsprobleme im Zusammenhang mit kritischen Infrastrukturen

Die Zeiten, als kritische Netzwerke von allgemeinen Unternehmensnetzwerken getrennt waren, sind Vergangenheit. Heute müssen Unternehmen kritische Netzwerke für Analysen und Pläne, kundenspezifische Entwicklungen, zum Schutz von Systemen sowie für vorgeschriebene Audits nach nützlichen Informationen durchsuchen. Darüber hinaus müssen sie Mitarbeitern, Vertragspartnern, Integratoren und Fachhändlern den Remote-Zugriff auf kritische Netzwerke erlauben. Auch sind Unternehmen zu dem Schluss gekommen, dass sie sich den ineffizienten und kostenträchtigen Ansatz, zwei Computer auf den Schreibtischen der Mitarbeiter stehen zu haben – einen für das kritische Netzwerk und den anderen für allgemeine Geschäftsvorgänge – nicht mehr leisten können. Daher wird oft vorgeschrieben, dass der Zugriff auf beide Systeme über ein und denselben Rechner erfolgen muss.

Was Unternehmen bei der Öffnung ihrer kritischen Netzwerke nicht immer ausreichend bedenken, ist die Leichtigkeit, mit der herkömmliche IT-Sicherheitsbedrohungen in diese Netzwerke gelangen können. Somit sind kritische Systeme nun den gleichen Sicherheitsbedrohungen ausgesetzt, die IT-Administratoren schon seit Jahren Kopfzerbrechen bereiten. Unglücklicherweise sind Viren, Trojaner, Würmer und Malware nur die Spitze des Eisbergs.

Angriffsarten:	<ul style="list-style-type: none"> • Datenabfang • Datenmanipulation • Denial-of-Service • Adressen-Spoofing • Unerwünschte Antworten • Übernahme von Sitzungen • Protokoll- / Paket-Fuzzing • Modifikation von Log-Daten • Unbefugte Kontrolle • Buffer Overflow • Versuche, mit Drohungen eines Angriffs auf das Netzwerk Geld zu erpressen
Arten des Missbrauchs:	<ul style="list-style-type: none"> • Datendiebstahl • Manipulation kritischer Daten • Beschädigung der Werksausstattung • Umkonfiguration der Steuerungseinstellungen • Änderung der Arbeitsanweisungen • Unbefugte Änderungen • Vorzeitiges oder vollständiges Herunterfahren des Werks • Manipulation von Sicherheitssystemen • Störung oder Zensur der Massenberichterstattung über wichtige Ereignisse
Arten der potenziellen Angreifer oder Bedrohungen:	<ul style="list-style-type: none"> • Personen, die Nervenkitzel suchen • Botnet-Besitzer • Computerkriminelle • Ausländische Geheimdienste • Phisher, Spammer und Spyware-Schreiber • Terroristen • Industriespione • Verärgerte Mitarbeiter • Auftragnehmer und andere vorübergehend Beschäftigte • Verbotene Software • Ungeprüfte oder ungesicherte Updates vom Anbieter • Fehlfunktionen der Software • Untaugliche und/oder veraltete Richtlinien • Reserve- oder Hilfssysteme, die nicht über das gleiche Schutzniveau wie die Hauptssysteme verfügen

Potenzielle Schäden:	<ul style="list-style-type: none"> • Beeinträchtigte Sicherheit der Standortbelegschaft, der Öffentlichkeit und der Umwelt mit potenziell schädlichen oder gar tödlichen Folgen • Auswirkungen auf die nationale Sicherheit • Produktivitätseinbußen oder Produktionsstopp an einem oder mehreren Standorten gleichzeitig • Schäden an Ausrüstung, deren Austausch Monate dauern kann • Freisetzung, Umleitung oder Diebstahl von Gefahrstoffen • Verstoß gegen gesetzliche Vorschriften • Produktkontamination • Straf- oder zivilrechtliche Haftung • Verlust von urheberrechtlich geschützten oder vertraulichen Daten • Beschädigung des Marken-Image oder Verlust des Kundenvertrauens
----------------------	---

Tabelle 1: Potenzielle Internetangriffe und Schäden an kritischen Infrastrukturen.

Nicht auf Sicherheit ausgelegt

Nach jahrelanger Abwehr von Computerkriminellen sind IT-Netzwerke in Unternehmen mittlerweile auf Sicherheit ausgelegt und verfügen über wirksame Schutzeinrichtungen für Desktops und LAN-Systeme. Die Geschichte kritischer Netzwerke jedoch ist nicht in ähnlicher Weise durch den Aufbau von Schutzmaßnahmen und die Abwehr von Angriffen geprägt. Da solche Systeme in der Regel isoliert waren, spielten Verfügbarkeit, Datenintegrität und Zuverlässigkeit eine viel wichtigere Rolle als Sicherheit.

Diese Umstände haben zu einigen ziemlich einmaligen Unterschieden geführt, die die Ausbringung von standardmäßigen Sicherheitslösungen auf kritischen Netzwerken erschweren. So führen beispielsweise Ausfallzeiten zum Einspielen von Patches oder zur Aktualisierung der Signaturdateien zu einem zwei bis sechs Minuten langen Denial-of-Service. Bei einem System mit einer Verfügbarkeitsvorgabe von 99,99999 Prozent würde nur eine dieser Aktualisierungen im Jahr bereits bedeuten, dass die Sollverfügbarkeit nicht mehr erreicht werden kann.

Kritische Infrastruktur-Netzwerke weisen unter anderem die folgenden besonderen Sicherheitsprobleme auf:

- Einspielung von Patches oder Aktualisierungen führt zu inakzeptablem Denial-of-Service
- Maßgeschneiderte Betriebssysteme sind oft veraltet und lassen sich nicht patchen
- Proprietäre Protokolle werden durch Standard-Firewalls nicht erkannt oder geschützt
- Infrastrukturtechniker sind in Sicherheitsfragen oft nicht so gut geschult wie ihre Kollegen im IT-Bereich
- Unkontrollierte Geräte können sich direkt in Netzwerke einklinken und sie kontrollieren
- Vertrauliche Daten sind an verschiedenen Orten im Netzwerk ohne Verschlüsselung oder Zugriffskontrollen gespeichert
- Der Zugriff auf mobile Geräte erfolgt über ungesicherte Drahtlos-Netzwerke

Das Problem ist real

Die Gefahr ist nicht nur theoretisch. Obwohl es kaum Berichterstattung hierzu gab, sind bereits seit einigen Jahren Fälle von Angriffen auf kritische Infrastrukturen aufgetreten, und die Tendenz ist steigend. Die folgenden Fälle sind aus den SANS NewsBites¹ für das letzte Quartal 2008 entnommen:

- Auf den Computersystemen zweier Unternehmen, die Waffen und Schiffe für die südkoreanische Armee herstellen, wurde Schadcode gefunden. In diesem Bereich ist besondere Wachsamkeit geboten, da Angreifer maßgeschneiderte Malware einsetzen könnten, um an geheime Daten von militärischer Relevanz zu gelangen.
- Der Software-Anbieter Citect hat die Schwere der Fehler in seinem SCADA-Produkt zunächst heruntergespielt. Nachdem jedoch Code veröffentlicht wurde, mit dem sich der Fehler ausnutzen ließ, ersetzte das Unternehmen den ursprünglichen Rat durch eine stärker formulierte Version. Einer der Redakteure bei SANS kommentierte: „Leider muss man SCADA-Händler in der Regel dazu zwingen, die Tragweite der Sicherheitsmängel und die Wichtigkeit der dazugehörigen Patches zu erwähnen.“
- Die Vereinigten Arabischen Emirate (VAE) gaben an, dass ein erfolgreicher Angriff auf ein Netzwerk durchgeführt wurde, das von Banken zur gemeinsamen Nutzung der Daten von Geldautomaten verwendet wird. Zu den betroffenen Banken zählten die Citibank, HSBC, Lloyds TSB, die Nationalbank von Abu Dhabi und Emirates NBD.
- Nach einem Bericht des Sonderprüfers des US-Finanzministeriums für Steuerverwaltung sind an das Netzwerk der US-Bundessteuerbehörde Internal Revenue Service mehr als 1.800 nicht genehmigte interne Web-Server angeschlossen. Aus dem Audit ging hervor, dass 2.093 Web-Server mit mindestens einer bekannten Sicherheitslücke in Verbindung mit dem IRS-Netzwerk standen.

- Unterstützer der Hamas konnten sich Zugriff auf einen israelischen Domain Registration Server verschaffen und mehrere Stunden lang Internetnutzer, die auf die Seiten Ynetnews und Bank Discount zugreifen wollten, auf einen Server in Japan umleiten, auf dem eine Propaganda-Seite gehostet war.

Auch einige weitere Exploits schafften es in die Nachrichten:

Weltbank mindestens sechsmal bestohlen

- Hacker waren in der Lage, über ein Jahr lang nach Belieben Daten aus dem Computernetzwerk der Weltbank zu stehlen. Wie viele Daten dabei tatsächlich gestohlen wurden, ist bis heute nicht bekannt. Im Juni/Juli 2008 hatten die Angreifer darüber hinaus beinahe einen Monat lang Zugriff auf das restliche Netzwerk der Weltbank. Insgesamt wurden seit Sommer 2008 mindestens sechs größere Angriffe – zwei davon mit der gleichen Gruppe chinesischer IP-Adressen – vorgetragen, der letzte davon im September 2008. (Quelle: <http://www.foxnews.com/story/0,2933,435681,00.html>)

Ehemaliger Mitarbeiter erst nach 46. Angriff gestoppt

- In Australien machte sich ein unzufriedener Mitarbeiter Schwachstellen eines Drahtlos-Netzwerks zunutze, um sich immer und immer wieder in das Steuersystem einer Wasserversorgungsbehörde zu hacken. Die ersten 20 erfolgreichen Angriffe wurden zunächst für mechanische oder elektrische Probleme mit dem Behördennetzwerk und/oder den dazugehörigen Mobilgeräten gehalten. Selbst nachdem bekannt wurde, dass es sich um einen Internetangriff handelte, war die Behörde nicht in der Lage, die Angriffe zu unterbinden. Zuletzt konnte der Hacker Pumpen außer Betrieb nehmen, Alarmmeldungen blockieren und die Kommunikation zwischen den Zentralrechnern und verschiedenen Pumpstationen zum Erliegen bringen. Der fünfundvierzigste Angriff hatte zur Folge, dass eine Pumpstation überlief, so dass das entweichende Abwasser ein Wohnviertel und einen Flutkanal verschmutzte. Weil das Unternehmen nicht über ausreichende forensische Technologien verfügte, war es über zwei Monate lang nicht in der Lage, die Angriffe zu stoppen. (Quelle: http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/)

Sicherheitsmaßnahmen für unnötig befunden

- Beamte eines Energieversorgungsunternehmens integrierten ein System zur geographischen Kartierung in das werkseigene Steuersystem. Sie führten eine Risikoanalyse durch und entschlossen sich, das Steuersystem direkt ans Internet anzubinden und keinerlei Firewalls oder andere Schutzmaßnahmen einzusetzen. Das Ergebnis war wenig überraschend: Innerhalb von Minuten wurde das Steuersystem mit einem Rootkit-Angriff kompromittiert und ausgeschaltet.

In einer normalen IT-Umgebung wäre dieser Angriff auf einige wenige Systeme beschränkt gewesen, und deren Wiederherstellung hätte nicht allzu lange gedauert – höchstens ein paar Stunden, um neue Laufwerks-Images aufzuspielen. Doch wie eingangs erwähnt, verfügen kritische Infrastruktursysteme nicht über die gleichen Schutzvorkehrungen und die gleiche Ausfallsicherheit wie IT-Systeme. In diesem Fall musste der Energieversorger zwei Wochen lang auf sein Steuersystem verzichten, und die Behebung des Schadens dauerte vier Mann-Monate. (Quelle: beim KEMA-Workshop 2004 vorgelegte Studie)

Zensur von politischen Protesten

- Im April 2008 wurden acht Webseiten des Senders Radio Freies Europa durch massive Denial of Service-Angriffe zwei komplette Tage lang ausgeschaltet, weil der Sender von Protesten weißrussischer Oppositionsgruppen anlässlich des Jahrestags der Tschernobyl-Katastrophe berichtete. Diese Art von „Just-in-Time“-Zensur ist immer häufiger zu beobachten, da „Hacktivist“ Internetangriffe dazu einsetzen, ihre politischen Ansichten vorzutragen. (Quelle: <http://www.rferl.org/featuresarticle/2008/4/83ebf181-e31e-474b-8238-889566a108bc.html>)

Remote-Zugriff ausgenutzt

Nachfolgend werden Fälle geschildert, in denen sich Fernzugriff als die Achillesferse erwies:

- 1994 wurde das kritische Netzwerk eines großen Wasser- und Energieversorgers im amerikanischen Phoenix (Arizona) geknackt. Auf die Computer wurde mithilfe eines DFÜ-Modems über ein Backup-System zugegriffen.
- 1997 wurde das Telefonnetz der Flugsicherung am Worcester Airport mithilfe eines DFÜ-Modems außer Gefecht gesetzt. Damit wurde die Telefonverbindung zum Kontrollturm, zum Flughafen-Sicherheitsdienst, zur Flughafen-Feuerwehr, zum Wetterdienst und zu den Fluglinien unterbrochen. Ebenfalls wurde die Landebahnbeleuchtung sowie die Telefonverbindung zu 600 Haushalten abgeschaltet.

Viren dringen in kritische Netzwerke ein

- Der Slammer-Wurm schlich sich auf verschlungenen Pfaden in das Kernkraftwerk Davis-Besse im US-Bundesstaat Ohio ein. Zunächst infiltrierte er das ungesicherte Netzwerk eines Auftragnehmers und schlich sich dann durch eine T1-Linie, die dieses Netzwerk mit dem Betriebsnetzwerk von Davis-Besse verband. Bei späteren Untersuchungen fand man heraus, dass diese T1-Linie eine von zahlreichen Wegen in das Betriebsnetz von Davis-Besse war, mit denen die Firewall der Anlage komplett umgangen werden konnten. Die Wiederherstellung des infizierten Systems dauerte vier Stunden und fünfzig Minuten, und bis auch die anderen wieder funktionierten, verstrichen sechs Stunden und neun Minuten.

Ein zweiter Vorfall mit dem Slammer-Wurm ereignete sich, als der Virus das kritische SCADA-Netzwerk einer Behörde ausschaltete, nachdem er von einem Remote-Computer aus über eine VPN-Verbindung in das LAN der Steuerzentrale gelangen konnte. In einem dritten Fall wurde der SCADA-Datenverkehr eines Energieversorgers unterbrochen, weil die hierfür benötigte Bandbreite von einem Telekommunikationsunternehmen geleast war, die dem Wurm zum Opfer fiel.

(Quelle: <http://www.securityfocus.com/news/6767>)

Die Lösung: Fünf wesentliche Möglichkeiten zum Schutz kritischer Infrastrukturen

Zum vollständigen Schutz kritischer Infrastrukturnetzwerke reichen Einzelprodukte nicht aus. Vielmehr ist eine Kombination von fünf wesentlichen, ineinandergreifenden Sicherheitsvorkehrungen erforderlich, um soliden Schutz durch umfassende Abwehrmaßnahmen sicherzustellen. Diese fünf Sicherheitsvorkehrungen sind:

1. Ausbringung von Echtzeitschutz
2. Abtrennung und Abschirmung kritischer Infrastrukturen von verbundenen Netzwerken
3. Kontrolle der Zugriffsberechtigungen und der Netzwerkaktivitäten
4. Schutz von Daten über kritische Infrastrukturen vor Datendiebstahl
5. Ausbringung eines zuverlässigen Schutzes ohne Beeinträchtigung der erforderlichen Verfügbarkeit, Integrität und Zuverlässigkeit

1. Ausbringung von Echtzeitschutz

Signaturbasierter Schutz ist ein wichtiger Bestandteil des reaktiven Bedrohungs-Managements und wirkt recht gut gegen Malware, die bereits katalogisiert und in Signatur-Datenbanken aufgenommen wurde. Wie aber verhält es sich mit brandneuer Malware, die noch nicht erkannt wurde? Wie sieht es bei gezielten Angriffen aus, die zu spezifisch oder schnelllebig sind? Sich rein auf signaturbasierte Lösungen zu verlassen, ist keine wirkungsvolle Strategie zur Abwehr von Malware-Angriffen.

Heutzutage arbeiten die Angreifer in Echtzeit. Daher gibt es einen erheblichen Zuwachs bei sogenannten Zero-Day-Angriffen, die die folgenden Eigenschaften aufweisen:

- Sie zielen auf Sicherheitslücken, für die es noch keine Patches gibt.
- Sie verwenden neue Viren-Codes, die in den Signaturdateien der Virenschutz-Software noch nicht enthalten sind.
- Sie sind nicht weit genug verbreitet, als dass es trotz des erheblichen Schadenspotenzials wirtschaftlich sinnvoll wäre, Patches zu entwickeln.
- Sie setzen vornehmlich auf Tarnung, d.h. sie wollen von Ihnen unbemerkt bleiben
- Sie verschwinden ebenso schnell, wie sie aufgetreten sind.

Echtzeit-Angriffe erfordern Echtzeit-Schutz

Sicherheitslösungen der neuesten Generation sind in der Lage, sowohl Angreifer als auch Angriffe unter die Lupe zu nehmen. Durch eine Untersuchung des Verhaltens von Akteuren im Internet ist es möglich, ihnen Reputationswerte zuzuweisen und sicherheitsrelevante Entscheidungen auf Grundlage derartiger Berechnungen zu treffen. Ähnlich wie eine Bank den Kredit-Score zu Rate zieht, um über die Vergabe eines Kredits an einen Hauskäufer zu entscheiden, kann mithilfe von weltweiten Reputationsauswertungen der Zugriff auf Internet-Auftritte je nach Reputation des jeweiligen Auftritts gewährt oder verweigert werden. Somit lässt sich ungeachtet der Angriffsart Schutz in Echtzeit bieten.

Die Bedrohung durch Zero-Day-Angriffe wird immer da sein. Aber mithilfe der globalen Reputationsanalyse lassen sich diese Risiken verringern, weil diese nicht nur Hintergrundinformationen über die Person und ihre Reputation bereitstellt, sondern auch über die Reputationswerte der Personen, mit denen die betreffende Person in Verbindung steht. Wenn Sie ein globales Reputationssystem mit einer gründlichen inhaltlichen Prüfung aller anderen Daten kombinieren, erhalten Sie viel umfassendere Informationen über Akteure, die versuchen, auf Ihr Netzwerk zuzugreifen. Ihre kritischen Infrastrukturen können so viel wirksamer geschützt werden.

2. Abtrennung und Abschirmung kritischer Infrastrukturen von verbundenen Netzwerken

Es lässt sich nicht leugnen: Heutzutage *müssen* Netzwerke miteinander verbunden sein. Allerdings muss der Datenverkehr über diese Netzwerke verwaltet und gesichert werden, um Risikofaktoren für einen erfolgreichen Angriff zu isolieren.

Erste Schutzstufe: Die Firewall

Bei der Entwicklung eines Sicherheitskonzepts für ein kritisches Netzwerk muss von Anfang an unbedingt darauf geachtet werden, dass es von sämtlichen nicht-kritischen Daten und Datenströmen abgetrennt und geschützt ist. Indem die Anzahl der ein- und ausgehenden Verbindungspunkte begrenzt wird, kann die Anfälligkeit des kritischen Netzwerks gegenüber Risiken minimiert werden. An den erforderlichen Verbindungspunkten jedoch ist eine genau für diesen Zweck konzipierte Vorrichtung zur Zugangssteuerung und Prüfung unverzichtbar. Die am häufigsten hierfür ausgebrachte Vorrichtung ist eine Firewall. Es gibt jedoch verschiedene Arten von Firewalls, die sich im Hinblick auf den von ihnen gebotenen Schutz stark unterscheiden.

- Firewalls mit statusbehafteter Paketprüfung (SPI), auch Paketfilter-Filterwalls – Diese Firewalls werden gemäß dem auf sieben Schichten basierenden OSI-Modell in der Vermittlungsschicht (Layer 3 – Network) betrieben und untersuchen jedes einzelne Datenpaket, das durch das Netzwerk übertragen wird. Die Firewall lässt nur Pakete durch, die zu einem bekannten Verbindungsstatus passen; alle anderen Pakete werden abgewiesen. Selbst Firewalls, die angeblich eine tiefgehende Paketprüfung durchführen, basieren normalerweise auf Signaturdateien, also einer rein reaktiven Technologie, mit der nur bereits bekannte Angriffsarten abgewehrt werden können. Einer Organisation, die kritische Infrastrukturen schützen muss, bietet eine SPI-Firewall (selbst mit Unterstützung in Form von Signaturdateien) keinen ausreichenden Schutz, da sie externen Clients einen direkten Austausch von Datenpaketen mit internen Anwendungen erlaubt. Diese Konstellation birgt das Risiko, dass Hacker Aufschlüsse über Schwachstellen der Anwendungen erlangen könnten, und ist daher weitgehend wirkungslos gegen neue, zielgerichtete und unbekannte „Zero Hour“-Angriffe.
- Firewalls im Anwendungs-Layer – Um kritische Anwendungen und betriebliche Abläufe wirksam zu ermöglichen und gleichzeitig Risiken durch gezielte Angriffe zu minimieren, ist eine Firewall erforderlich, die die Anwendungen im Anwendungs-Layer (Layer 7 nach dem OSI-Modell) filtert und prüft. Mithilfe von statusbehafteter Paketprüfung kann bestimmt werden, welche Art von Netzwerkprotokoll (TCP, UDP, ICMP usw.) über jeden Port gesendet wird, aber Firewalls im Anwendungs-Layer können darüber hinaus analysieren und festlegen, für welche Anwendung die jeweiligen Protokolle verwendet werden. So sollte beispielsweise ein Filter im Anwendungs-Layer in der Lage sein, HTTP-Datenverkehr für den Zugriff auf von Ihnen gehosteten Webseiten von über den gleichen Port gesendetem SSH-Datenverkehr zu unterscheiden, mit dem versucht wird, gegen Ihre Sicherheitsrichtlinien unerwünschten Datenverkehr in Ihr Unternehmen und vom Unternehmen nach außen zu schmuggeln. Eine Firewall mit statusbehafteter Paketprüfung kann diese beiden Arten von Datenverkehr nicht unterscheiden und behandelt sämtlichen über einen Port ein- und ausgehenden Datenverkehr gleich.

Firewalls im Anwendungs-Layer ermöglichen auch die Verwendung mehrerer anwendungsspezifischer Proxys über eine einzelne Firewall. Die Proxys sind zwischen Client und Server geschaltet und leiten Daten zwischen diesen beiden Endgeräten hin und her. Verdächtige Daten werden dabei blockiert, und es herrscht niemals direkte Kommunikation zwischen Client und Server. Da Proxys im Anwendungs-Layer anwendungsbewusst sind, kommen sie besser mit komplexen Protokollen zurecht.

Die besten Firewalls im Anwendungs-Layer sind solche, die die genannten tiefgreifenden Prüfungen durchführen und die folgenden Eigenschaften aufweisen:

- Port-Zugriffssteuerung auf Grundlage eines positiven Sicherheitskonzepts (d. h. Verweigerung aller Zugriffe außer den ausdrücklich erlaubten)
- Betrieb auf Gigabit-Geschwindigkeit, so dass die Verfügbarkeits- und Integritätsvorgaben für das Steuersystem eingehalten werden
- Speziell auf Steuersysteme ausgelegte Funktionen
- Bereitstellung eines wirklich geschützten Betriebssystems – und nicht nur eines modifizierten Standard-Systems – das sich gegen Angriffe verteidigen, Root-Zugriffe vermeiden oder beseitigen und eine Berechtigungs eskalation oder die Ausführung von beliebigem Code durch Außenstehende unterbinden kann
- Beseitigung aller uneingeschränkten Rechte und befremdlicher Dienste einschließlich einer Trennung des Netzwerk-Stacks und Kontrolle der Berechtigungen von Super-Usern bei gleichzeitiger Bereitstellung von Auslösern zur Erkennung von Eindringversuchen
- Bereitstellung einer einfach auszubringenden und zu verwaltenden Architektur mit zentraler Richtlinienvorgabe und Berichterstattung sowie starken Forensik-Funktionen
- Automatische Herausfilterung von Verbindungen aus verdächtigen oder im normalen Betrieb nicht erforderlichen Orten
- Scannen von verschlüsseltem Datenverkehr (HTTPS, SSL, SSH, SFTP, SCP usw.) zur Aufdeckung und Abwehr von versteckten Angriffen
- Bereitstellung strikter branchenspezifischer und staatlicher Zertifizierungen und Referenzen (eine Zertifizierung nach Common Criteria EAL4+ gilt als empfohlenes Minimum)
- Bereitstellung einer Sicherheits-Architektur, die langfristig und nachweislich niemals überwunden oder gehackt wurde

Als Fazit lässt sich festhalten, dass das kritische Netzwerk von allen Seiten geschützt sein muss. Egal, ob Unternehmens-LAN, Reserve-Rechenzentrum, Drittanbieter oder das Netzwerk eines unabhängigen Systembetreibers: Alles, was einen Berührungspunkt mit dem kritischen Netzwerk hat, muss mit einer wirkungsvollen „Defense in Depth“-Strategie sowie mit der richtigen Firewall im Anwendungs-Layer als erster Verteidigungslinie gesichert werden.

Zweite Schutzstufe: Intrusion Prevention

Eine starke Verteidigung erfordert Wachsamkeit auf mehreren Ebene. Zum Schutz der kritischen Infrastruktur ist ein Intrusion Prevention-System (IPS) von wesentlicher Bedeutung.

Ein IPS ist normalerweise so ausgelegt, dass es im Netzwerkbetrieb nicht wahrgenommen wird. In der Regel beanspruchen IPS-Produkte keine IP-Adresse im geschützten Netzwerk, können aber auf verschiedene Art und Weise direkt auf jegliche Art von Datenverkehr reagieren. Die möglichen Reaktionen umfassen das Verwerfen von Paketen, das Zurücksetzen von Verbindungen, die Ausgabe von Warnmeldungen und sogar das Isolieren von Eindringlingen. Die IPS-Technologie ermöglicht tiefere Einblicke in den Netzwerkbetrieb, indem sie Informationen über übermäßig aktive Hosts, fehlgeschlagene Anmeldeversuche, unangemessene Inhalte und viele andere Funktionen der Netzwerkschicht und des Anwendungs-Layers liefert.

Der wichtigste einzelne Gradmesser für die Wirksamkeit des Netzwerkschutzes ist die Fähigkeit, kritische Unternehmensressourcen vor Angreifern zu schützen, bevor diese eine Schwachstelle ausnutzen können. Die meisten IPS-Anbieter geben zwar an, dass sie für Schutz sorgen, sobald eine neue Schwachstelle bekanntgegeben wird, aber nicht alle bieten auch im kritischen Zeitraum bis zum Bekanntwerden einer Schwachstelle den gleichen Schutz. Das liegt daran, dass mehrere Schwachstellen – jede mit einer einzelnen Bezeichnung – meist in einer einzigen Schwachstellenmeldung zusammengefasst werden. Wenn also ein Anbieter angibt, die Schwachstellen aus dieser Meldung abgedeckt zu haben, können Sie sich nicht immer darauf verlassen, dass der Schutz auch wirklich alle einzeln bezeichneten Schwachstellen umfasst.

Eine für kritische Infrastrukturen geeignete IPS-Lösung muss in der Lage sein, mit derart hoher Geschwindigkeit zu arbeiten, dass Verfügbarkeitsvorgaben eingehalten werden. Im Falle der meisten Unternehmen bedeutet dies eine Geschwindigkeit von mehreren Gigabit pro Sekunde. Darüber hinaus sollte eine geeignete IPS-Lösung auch die folgenden Fähigkeiten aufweisen:

- Schutz Ihres Unternehmens vor bekannten, Zero-Day- und verschlüsselten sowie DoS- und DDoS-Angriffen, Syn-Flood-Attacken und Bedrohungen wie Spyware, Schwachstellen in Voice-over-IP (VoIP)-Produkten, Botnetzen, Malware, Würmern, Trojanern, Phishing und Peer-to-Peer-Tunnelangriffen.
- Erhöhte Genauigkeit durch den Einsatz mehrerer fortschrittlicher Erkennungsverfahren auf Grundlage von Anomalien in Signaturen, Anwendungen und Protokollen, Algorithmen zur Erkennung von Shell-Code und Schutzfunktionen der neuesten Generation gegen DoS- und DDoS-Angriffe.

- Durchsuchung von über 100 Protokollen und Prüfung von mehr als 3.000 qualitativ hochwertigen Signaturen mit mehrfachen Attributen und Auslösern sowie statusbehafteter Überprüfung des Datenverkehrs
- Präventive, sofort einsatzbereite Abwehr von hunderten von Angriffen mit vorkonfigurierten „Zur Sperrung empfohlen“-Richtlinien
- Kontinuierliche Bereitstellung von Bedrohungs-Updates durch weltweite Forschungsteams rund um die Uhr

3. Kontrolle der Zugriffsberechtigungen und der Netzwerkaktivitäten

Die Möglichkeit eines Remote-Zugriffs kann aus verschiedenen geschäftlichen Gründen unverzichtbar sein:

- Industrieunternehmen, die Daten oder Ressourcen gemeinsam nutzen müssen
- Anbieter, die kritische Systeme überwachen und aktualisieren müssen
- Mitarbeiter, die räumlich von Ressourcen getrennt sind
- Auftragnehmer oder vorübergehend Beschäftigte, die Zugang zu entfernten Ressourcen benötigen
- In verbundenen Systemen tätige Mitarbeiter, die Zugang benötigen, um verfügbare Kapazitäten zu bestimmen

Aus all diesen Gründen wird der Remote-Zugriff eine unausweichliche Gegebenheit im Geschäftsbetrieb bleiben – und eine Schwachstelle. Eine „Defense in Depth“-Strategie kann jedoch dazu beitragen, Sicherheitsprobleme im Zusammenhang mit Remote-Zugriffen in den Griff zu bekommen.

Eine umfassende „Defense in Depth“-Strategie besteht aus vier Kernelementen:

- **Authentifizierung der PERSON** – Vorrichtungen für strikte Zwei-Faktor-Authentifizierung wie Tokens oder Einmal-Passwort-Generatoren bieten wichtigen Schutz für kritische Systeme. Ebenso wie eine Bank nicht im Traum daran denken würde, einem Kunden über einen Geldautomaten ohne Bankkarte und PIN-Zugriff auf ihre Geldbestände zu gewähren, können Versorgungsunternehmen ohne ähnliche Schutzmaßnahmen keinen Zugriff auf Kraftwerke erlauben.
- **Authentifizierung der ANLAGEN** – Versorgungsunternehmen müssen wissen, von welcher Anlage aus der Zugriffsversuch erfolgt und ob die Nutzung dieser Anlage richtlinienkonform ist. Die Remote-Authentifizierung von Anlagen ermöglicht es einem Unternehmen, von Remote-Anwendern einsetzbare Systeme genau zu spezifizieren. Im Falle des unzufriedenen Australiers, der sich Schwachstellen in einem Drahtlos-Netzwerk zunutze machte, um sich immer wieder in eine Abwasserbehörde zu hacken (siehe Seite 6), dienen nicht autorisierte Anlagen als Ausgangspunkt für den Hack ins System. Hätte die Behörde ein stimmiges Konzept zur Remote-Authentifizierung von Anlagen eingesetzt, wären die Zugriffsversuche fehlgeschlagen.
- **Authentifizierung der INHALTE** – WLAN- und DFÜ-Modems sind die am häufigsten genutzten Kommunikationskanäle an Remote-Standorten, und sie weisen gut dokumentierte Schwachstellen auf. Die jüngsten Angriffe haben den Umstand ausgenutzt, dass viele Sicherheitslösungen verschlüsselte Kommunikation übersehen, und so waren Hacker in der Lage, durch das Verstecken ihrer Angriffe in verschlüsselten Paketen durch Firewalls und Gateways zu schlüpfen. Der einzige wirkliche Schutz hiergegen ist der Einsatz von Schutzvorkehrungen, die Datenverkehr entschlüsseln, Sicherheitsprüfungen darauf anwenden und ihn daraufhin je nach Bedarf wieder verschlüsseln.

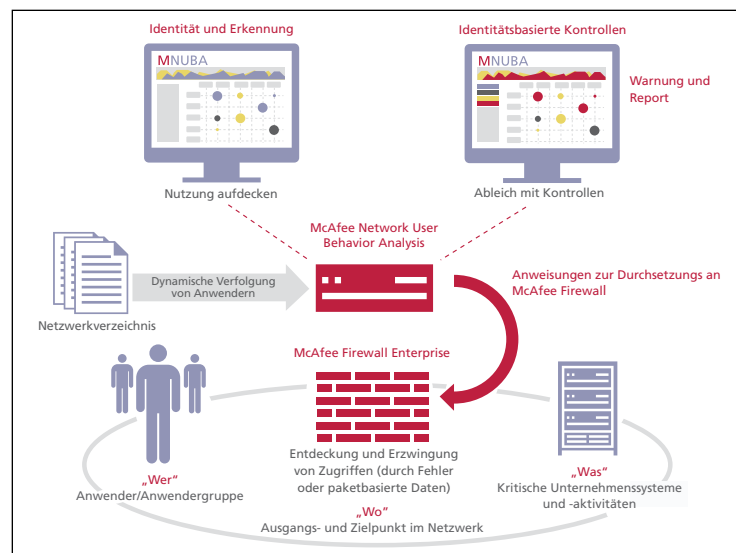


Abbildung 2: Netzwerkweite Überwachung und/oder Sperrung in Echtzeit.

- *Überwachung der AKTIVITÄTEN* – Wenn Maßnahmen zur Zugriffssteuerung aktiv sind, besteht der nächste Schritt in der Überwachung von Aktivitäten im Netzwerk. Es ist von wesentlicher Bedeutung, zu verstehen, welche Personen worauf zugreifen und was sie nach erfolgreichem Zugriff tun.

Im Zusammenhang mit dem letzten Punkt „Überwachung der Aktivitäten“ ist ein aktuelles Beispiel interessant, das sich bei Shell Oil ereignete. Dort griff ein autorisierter Auftragnehmer bei Arbeiten vor Ort auf eine Datenbank zu, die persönliche Daten über die meisten aktuellen und ehemaligen Shell-Mitarbeiter enthielt. Shell hat festgestellt, dass die Sozialversicherungsnummern von Mitarbeitern in vier Fällen dazu verwendet wurden, gefälschte Arbeitslosmeldungen einzureichen. Hierbei handelt es sich offenbar um einen Fall, in dem ein autorisierter Anwender mit gültigen Zugriffsrechten auf nicht zulässige, unautorisierte Weise mit vertraulichen Daten umgegangen ist. In einem solchen Fall hilft reine Zugriffssteuerung nicht, und wenn nur derart kleine Datenmengen abgerufen werden, sind unter Umständen auch eine Überwachung der Datenbank-Aktivitäten und Warnmeldungen zum Schutz vor Datenverlusten nicht wirksam. (Quelle: http://www.theregister.co.uk/2008/10/07/shell_oil_database_breach/)

Was hätte also in diesem Fall funktioniert? Eine Kombination aus Echtzeit-Überwachung der Anwender-Aktivitäten und Sperrfunktionen ermöglicht es, die Aktivitäten einzelner Anwender zu kontrollieren und skrupellosen Taten vorzubeugen.

4. Schutz von Daten über kritische Infrastrukturen vor Datendiebstahl

Nicht nur der Schutz der Anlagen selber ist extrem wichtig, da alleine Informationen über diese kritischen Anlagen von Computerkriminellen schon dazu genutzt werden können, genau darauf zugeschnittene Angriffe zu planen. Auf Unternehmenssystemen gespeicherte vertrauliche Informationen wie Betriebsabläufe, Netzwerk-Topologien, Grundrisse von Rechenzentren, Aufstellungspläne, Katastrophen- und Notfallschutzpläne, sicherheitsrelevante Konfigurationsdaten und technische Zeichnungen müssen anhand von Konzepten wie „Least Privilege“ (minimale Rechtevergabe) und „Need to Know“ geschützt werden, die den meisten Sicherheitsexperten vertraut sind.

Jeder Plan zur Verhinderung von Datendiebstahl muss die folgenden drei „Zustände“ von Daten berücksichtigen:

- *Gespeicherte Daten* – in freigegebenen Dateien, Repositories usw. gespeicherte Informationen
- *Verwendete Daten* – Daten, die gerade aktiv von Personen oder Systemen verwendet werden
- *Bewegte Daten* – Daten, die innerhalb des Unternehmens oder über das Internet übertragen werden

Der Schutz bewegter Daten ist die kniffligste Aufgabe. Heute sind jedoch ausgeklügelte Technologien verfügbar, mit denen sich vertrauliche Daten auch in der Übertragung durchs Web oder über E-Mail erkennen lassen und mit denen deren Sicherheit durch Richtliniendurchsetzung am Gateway verwaltet werden kann. Die richtige Lösung zum Schutz vor Diebstahl bewegter Daten sollte in der Lage sein, bei der Entdeckung vertraulicher Daten automatisch eine oder alle der folgenden Maßnahmen zu treffen:

- Verwerfen
- Blindkopieren
- Ersetzen
- Die Nachricht ganz oder teilweise verwerfen
- Als eingefügte Nachricht oder Anhang weiterleiten
- Isolieren
- Umleiten
- Voranstellen
- Protokollieren
- Zum sicheren Versand verschlüsseln
- Betreffzeile austauschen
- Mitarbeiter, Vorgesetzte oder Compliance-Verantwortliche benachrichtigen
- Archivieren
- Benutzer über Regeln aufklären

Außerdem sollten Ausbringungen zum Schutz vor Datendiebstahl in der Lage sein, Aktionen so zu kombinieren, dass sich daraus Richtlinien ergeben, nach denen sich eine Nachricht sowohl verschlüsseln als auch an einen Vorgesetzten senden, blockieren oder archivieren lässt.

Datenschutzlösungen für kritische Netzwerke sollten eine zentrale Verwaltung, Auditierung, Reporting, Zwischenfall- und Fallverwaltung sowie eine detaillierte Forensik in Kombination mit innovativen Lernfunktionen beinhalten. Lösungen mit diesem Funktionsumfang können unabhängig vom Zustand der Daten verlässlichen Schutz bieten.

5. Ausbringung eines zuverlässigen Schutzes ohne Beeinträchtigung von Verfügbarkeits-, Integritäts- und Zuverlässigkeitsanforderungen

Bei kritischen Infrastrukturen muss sich die Sicherheit problemlos mit den Anforderungen an Verfügbarkeit, Integrität und Zuverlässigkeit vertragen. Aus diesem Grund können viele Verfahren zur Aktualisierung und Wartung des Sicherheitssystems, die normalerweise auf Unternehmenssystemen ausgebracht werden, bei kritischen Infrastrukturen keine Anwendung finden. Tatsächlich ist bei kritischen Infrastruktursystemen das Ausräumen zwischen Sicherheit und Nutzbarkeit extrem knifflig und wirft einige einzigartige Herausforderungen bei der Konzipierung des Netzwerks auf. Damit die Sicherheitsmaßnahmen auf kritischen Systemen wirken, müssen sie folgende Eigenschaften und Funktionen bieten:

Trusted Security-Modell

Ausgangspunkt ist ein „positives“ Sicherheitskonzept, bei dem alle nicht ausdrücklich zulässigen Handlungen verweigert werden. Daraufhin werden Reputationswerte auf Grundlage umfangreicher Verhaltensanalysen berechnet. Diese Kombination bietet die präziseste Echtzeit-Gefahrenabwehr auf dem Markt.

- Automatische Aktualisierungen, für die kritische Anlagen nicht vom Netz genommen werden müssen
- Unterstützung der langen Lebensdauer kritischer Anlagen
- Minimale Erfordernis von umfangreichen Tests und Ausfallzeiten vor dem Einspielen von Patches
- Schutz vor noch unbekanntem Bedrohungen
- Vorbeugung gegen Schwachstellen durch Berechtigungseskalation
- Unterstützung der für kritische Netzwerke speziellen und relevanten Signaturen
- Ausübung der Sicherheitsfunktionen bei so hoher Geschwindigkeit, dass die Netzwerkleistung nicht beeinträchtigt wird
- Ausbringung eines Trusted Security-Modells, das auf Reputationsbewertungen und gründlichem Verständnis der Anwendungen beruht

Nach sämtlichen Standards für kritische Infrastrukturen sind auch detailgenaue Forensik-Funktionen erforderlich, mit denen Vorfälle erkannt und Pläne zur Vermeidung zukünftiger Angriffe ausgebracht werden können. Gute Sicherheitsgeräte sollten in der Lage sein, Angriffsversuche in Echtzeit zu erkennen, sie abzuwehren und gleichzeitig Sicherheits-Administratoren mit detaillierten Warnmeldungen zu versorgen. Wenn diese strikten Sicherheitsmaßnahmen in der eingangs erwähnten australischen Wasseraufbereitungsanlage in Kraft gewesen wären, hätte man den Hacker bei seinem ersten Versuch abgewehrt, nicht erst beim sechsvierzigsten.

McAfee-Produkte und -Technologien für den Schutz kritischer Infrastrukturen

Unser Sortiment preisgekrönter Sicherheitsprodukte ist den speziellen Anforderungen zum Schutz kritischer Infrastrukturen gewachsen. McAfee kann auf langfristige Erfahrung im Schutz der wichtigsten Netzwerke und Daten der Welt zurückblicken. McAfee stellt seit 14 Jahren Sicherheitslösungen bereit, und bis jetzt ist noch kein McAfee-Gerät gehackt oder kompromittiert worden. Ebenso musste McAfee noch nie außer der Reihe einen Notfall-Sicherheitspatch für ein Firewall-Produkt herausgeben.

Darüber hinaus bietet McAfee branchenweit führenden Support rund um die Uhr, der Probleme zuverlässig und schnell löst. Die meisten Kunden werden innerhalb von Minuten direkt mit einem Experten verbunden, egal zu welcher Tages- oder Nachtzeit ein Problem auftritt. Auch können Sie auf die Beratungskompetenz von McAfee Professional Services zurückgreifen, damit Sie weniger Zeit für die Ausbringung benötigen und sicherstellen können, dass die Produkte optimal auf Ihre individuellen Bedürfnisse abgestimmt sind, damit sie sich schneller amortisieren und die bestmögliche Rendite erzielen.

McAfee TrustedSource

TrustedSource™ dient als Informationsquelle für alle McAfee Gateway-Sicherheitsprodukte und stellt damit die erste Verteidigungslinie dar. Es bietet einen umfassenden Überblick über die Reputation jedes Akteurs, der sich mit einer anderen Stelle im Internet in Verbindung setzt oder Daten dorthin liefern möchte. Dieses Wissen bietet den Vorteil, dass Angriffe unabhängig davon, ob sie bereits zuvor versucht wurden oder nicht, abgewehrt werden können, bevor sie Schaden anrichten.

Mithilfe einer Datenquelle von zehntausenden von Gateway-Sicherheits-Appliances in aller Welt verfolgt TrustedSource die Eigenschaften hunderter Milliarden Nachrichten und des damit einhergehenden Web-Datenverkehr über viele Jahre hinweg. Mit der Unterstützung durch ein auf Malware-Erkennung spezialisiertes Labor auf Weltklasse-Niveau kann TrustedSource schädliche Inhalte mühelos erkennen und sie auf die IP-Adresse zurückverfolgen, von der sie ausgesendet wurden.

TrustedSource ist so effektiv, dass es schädliche Verhaltensweisen regelmäßig schon Wochen vor einem tatsächlichen Angriff prognostiziert – und das mit einer Genauigkeit von 99 Prozent. Darüber hinaus geschehen diese Analysen „in the cloud“, also ohne Signatur- oder Datei-Aktualisierungen und ohne Ausfallzeiten. Und da TrustedSource sehr ausgereift ist und sich als akkurat und zuverlässig bewährt hat, sind False-Positives praktisch kein Thema mehr.

McAfee Firewall Enterprise kann ohne Ausfallzeiten aktualisiert werden, hält dreimal länger als andere Firewalls und bietet Echtzeitschutz gegen noch unbekannte Bedrohungen.

McAfee Firewall Enterprise

McAfee Firewall Enterprise (Sidewinder) ist eine multifunktionale Firewall im Anwendungs-Layer, die von den am stärksten sicherheitsbewussten Unternehmen und Regierungsstellen der Welt eingesetzt wird. McAfee Firewall Enterprise ist nach Common Criteria EAL4+ zertifiziert – hierbei handelt es sich um die höchste Zertifizierung, die ein Firewall-Produkt jemals erhielt. McAfee Firewall Enterprise wird zwischen kritischen Infrastrukturen und dem IT-Netzwerk des Unternehmens installiert und stellt sicher, dass jeglicher an kritischen Netzwerken ein- und ausgehender Datenverkehr zulässig, vertrauenswürdig und sicher ist.

McAfee Firewall Enterprise schützt kritische Netzwerke dank der folgenden Eigenschaften und Funktionen:

- *Trusted Security-Modell* – Eine Kombination aus Reputationsanalyse und einem „positiven Sicherheitsmodell“, bei dem grundsätzlich alle Inhalte als nicht vertrauenswürdig gelten, die nicht ausdrücklich als vertrauenswürdig ausgewiesen wurden. Ein Trusted Security-Modell ist das einzige Sicherheitsmodell, das sowohl vor bekannten als auch vor unbekanntem Zero-Hour-Angriffen schützen kann. Da McAfee Firewall Enterprise komplett auf das Trusted Security-Modell abgestimmt ist, kann das Produkt automatisch große Mengen an schädlichem Datenverkehr bereits auf Verbindungsebene verwerfen, ohne dass Signaturen oder Dateien aktualisiert werden müssen.
- *Schutz durch Geolocation* – McAfee Firewall Enterprise kann anhand der geographischen Herkunft einer Anfrage die anzuwendende Sicherheitsstufe festlegen. Wenn die Anfrage aus einem Land stammt, das als verdächtig bekannt oder nach Unternehmensrichtlinien nicht zulässig ist, kann McAfee Firewall Enterprise automatisch strengere Authentifizierungsanforderungen hinzufügen oder zusätzliche Prüfungen im Anwendungs-Layer und/oder auf Signaturrebene erstellen, um noch mehr Sicherheit zu bieten. So lässt sich beispielsweise ein Phisher davon abhalten, von ihm gestohlene Anmeldeinformationen erfolgreich auszunutzen. Durch höhere Sicherheit aufgrund des geographischen Standorts lässt sich die Anfälligkeit eines Unternehmens allein dadurch senken, dass Datenverkehr aus Ländern, in denen es keine Geschäfte tätigt, einfach blockiert wird. Dies führt nebenher zu Einsparungen durch geringere Verarbeitungszeiten und weniger Bandbreitenbedarf.

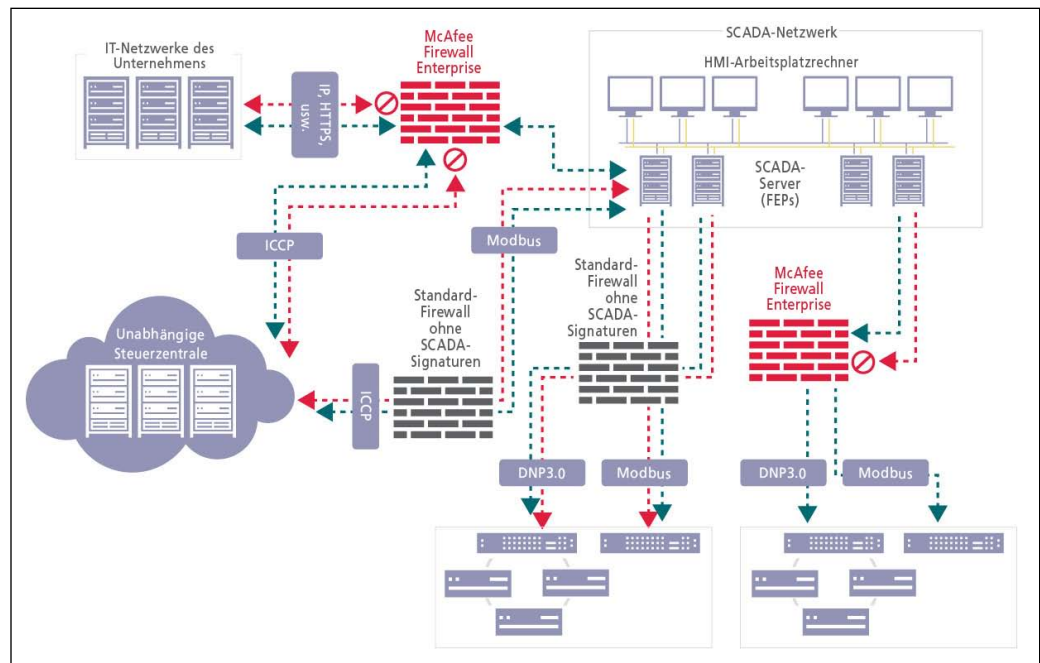


Abbildung 3: McAfee Firewall Enterprise schützt SCADA-spezifische Protokolle.

- *SCADA-spezifische Protokolle* – Herkömmliche Firewalls schützen nur in der IT häufig vorkommende Protokolle wie TCP/IP, HTTP, HTTPS und FTP. Sie können dagegen nicht vor Angriffen schützen, die ganz spezifisch auf SCADA-Netzwerke abgestimmt sind. McAfee Firewall Enterprise unterstützt Modbus, DNP 3.0 und ICCP, also wichtige SCADA-spezifische Protokolle, die bei kritischen Infrastruktur-Netzwerken zum Einsatz kommen. Durch die Einbeziehung von Signaturen für diese drei Protokolle lässt sich mit McAfee Firewall Enterprise sicherstellen, dass Steuersysteme gegen nicht autorisierte Eindringlinge, Denial-of-Service-Angriffe, Versuche der Kontrollübernahme über die Ausstattung und unbefugte Verwendung geschützt sind.
- *Vorbeugender Schutz vor Angriffen und Forensik* – McAfee Firewall Enterprise kann Schwachstellen mit Berechtigungs eskalation automatisch vorbeugen. Es verfügt über die Anwendungs-Proxys, die erforderlich sind, um die speziellen Anforderungen von Steuersystemen und Skalen ausreichend zu kennen, so dass keine Leistungseinbußen an kritischen Systemen auftreten. Darüber hinaus bietet McAfee Firewall Enterprise detaillierte Alarm-, Reporting- und Forensik-Funktionen, um Angriffsversuche zu erkennen. Es kann sie daraufhin abwehren, den Sicherheits-Administrator warnen und die zur Dokumentierung des Vorfalls erforderlichen Reports generieren. Mithilfe der Reporting-Option lassen sich alle McAfee Firewall Enterprise-Appliances im ausgedehnten Netzwerk zentral steuern, so dass sie sich von einem Punkt aus überblicken und verwalten lassen.



Abbildung 4: McAfee Firewall Reporter stellt eine zentrale Datenquelle für tausende von McAfee Firewall Enterprise- und McAfee UTM Firewall-Appliances dar.



Abbildung 5: McAfee Firewall Enterprise verfügt über die höchste Common Criteria-Zertifizierung.

- *Schutz im Anwendungs-Layer* – McAfee Firewall Enterprise ist die weltweit zuverlässigste Firewall im Anwendungs-Layer. In 14 Jahren musste niemals ein Notfall-Patch bereitgestellt oder eine Sicherheitswarnung ausgegeben werden. Darüber hinaus können McAfee Firewall Enterprise-Appliances 8 bis 12 Monate lang ununterbrochen und ohne jegliche Ausfallzeit in Betrieb bleiben.

Bevorzugte Wahl für kritische Infrastrukturen

McAfee Firewall Enterprise ist aus den folgenden Gründen seit über 14 Jahren die bevorzugte Wahl zum Schutz kritischer Infrastrukturen:

- Bereitstellung eines abgesicherten Betriebssystems, das noch niemals gehackt oder kompromittiert wurde
- Noch kein Notfall-Sicherheitspatch oder eine Betriebsunterbrechung aufgrund einer Schwachstelle erforderlich
- Verwendung eines Trusted Security-Modells zur Kombination positiver Sicherheit mit fortschrittlichem Schutz auf Reputationsbasis
- Prüfung von über 2,7 Gigabit pro Sekunde im Anwendungs-Layer
- Einfache Ausbringung und Verwaltung; neue Regeln können in wenigen Minuten hinzugefügt werden
- Ausgefeilte Geolocation-Analyse
- Unterstützung von ICCP, Modbus und DNP 3.0 mit SCADA-spezifischen Signaturtypen
- Scannen von verschlüsseltem Datenverkehr (HTTPS, SSL, SSH, SFPT, SCP usw.) zur Aufdeckung und Abwehr von versteckten Angriffen
- Selbstschutz durch patentierte Type Enforcement-Technologie, die die Installation von schädlicher Software oder die Koordinierung eines Buffer Overflow-Angriffs sowie andere bekannte oder unbekannte Angriffsarten unmöglich macht

- Verhinderung der Ausführung von fremder Software durch Beseitigung aller uneingeschränkten Rechte und befremdlichen Dienste
- Vollständige Trennung zwischen Anwendungen und dem Betriebssystem sowie zwischen den Anwendungen selbst
- Zertifiziert nach Common Criteria EAL4+
- Bereitstellung einer Sicherheitsarchitektur mit langer und erfolgreicher Einsatzhistorie in kritischen Infrastruktur-Netzwerken

McAfee Network IPS

McAfee Network IPS (ehemals IntruShield) ist eine zuverlässige Echtzeit-IPS-Lösung, die Ihnen einen Überblick darüber bietet, durch wen oder was Ihr Netzwerk und Ihre Systeme gefährdet werden und was Sie dagegen unternehmen müssen. Mit McAfee Network IPS kann die Zeit zwischen der Erkennung eines Angriffs und der endgültigen Behebung eines Problems erheblich verkürzt werden.

McAfee Network IPS sorgt für intelligentere Netzwerksicherheit, da es mit Ihrer Sicherheits-Infrastruktur zusammenarbeitet und sich in McAfee ePolicy Orchestrator®(ePO™), McAfee Network Access Control Module, und McAfee Vulnerability Manager integriert, um lückenlosen Schutz zu bieten.

So erhalten Sie auf Knopfdruck einen zentralen Überblick über Ihr Netzwerk und Informationen über die Relevanz von Bedrohungen und Risiken. Alles zusammen bringt Ihnen priorisierte, einschlägige Informationen, die es McAfee Network IPS ermöglichen, die drängendsten Probleme aufzugreifen.

Das Portfolio der leistungsfähigen und skalierbaren McAfee Network IPS-Appliances bietet die beste derzeit auf dem Markt erhältliche Lösung für ausfallsfreie Sicherheit und Portdichte. Darüber hinaus zeichnen sich McAfee Network IPS-Appliances auch in weit verteilten Ausbringungen durch einfache Steuerung, Konfiguration, Verwaltung und Überwachung mithilfe des McAfee Network IPS Managers aus.

McAfee Network IPS nutzt sowohl Signaturen als auch Heuristik zur Erkennung von bekannten Bedrohungen als auch Zero-Day-Angriffen. Während andere Anwender zur Erkennung von Angriffen auf einfache Musterübereinstimmungen setzen, verwendet McAfee Network IPS innovative und komplexe Zustandsmaschinen, um Angriffe im gesamten Datenverkehr zu erkennen. Mit derart umfassenden Prüfungen sowie leistungsfähigen und aufwendigen Decodern auf Grundlage spezialisierter Hardware-Komponenten schützt McAfee Network IPS selbst anspruchsvollste Ausbringungen ohne Einbußen bei Prüfgenauigkeit oder Systemleistung.

Das integrierte Intrusion Detection System (IDS), IPS und die Firewall-Systeme von McAfee Network IPS bieten überlegene Erkennungsgenauigkeit zur wirkungsvollen Überwachung, Erkennung, Auswertung und Abwehr von unzulässigem oder schädlichem Datenverkehr. Detaillierte Richtlinienkontrolle, eine robuste, genau auf ihren Einsatzzweck abgestimmte Hardware-Plattform und die virtuelle IPS-Architektur ermöglichen die effiziente Ausbringung und Wartung dieser Produkte sowie die Erstellung genauer Richtlinien für jedes einzelne Netzwerksegment. McAfee ePolicy Orchestrator stellt zentrale Schwachstellenbewertungs-, Verwaltungs- und Reporting-Funktionen bereit und bewirkt so einen noch flüssigeren Betrieb der Netzwerksicherheitssysteme sowie ein verbessertes Patch-Management.

McAfee UTM Firewall

McAfee UTM Firewall (ehemals SnapGear®) ist die ideale „All-in-One“-Firewall für Remote-Substations, Zweigstellen und Zugangspunkte für Dritte. Sie authentifiziert Remote-Geräte, die eine Verbindung mit dem Hauptrechenzentrum oder dem Hub anfragen. Darüber hinaus enthält Sie zahlreiche Sicherheitsfunktionen und bietet:

- Zentrale Verwaltung
- Zertifizierung für den Unternehmenseinsatz
- Virenschutz
- Intrusion Detection und Prevention
- Integration in TrustedSource
- Management von Sicherheitsvorfällen

Mithilfe des integrierten Modems kann die McAfee UTM Firewall auch in Drahtlos-Netzwerken zur Authentifizierung von Systemen eingesetzt werden, über die ein Zugriff auf kritische Anlagen angefragt wird. McAfee UTM Firewall ist eine kostengünstige Ergänzung für McAfee Firewall Enterprise (Sidewinder). Beide können über das McAfee Firewall Enterprise Control Center (CommandCenter) zentral verwaltet werden.

McAfee Network IPS wehrt mit backbone-tauglicher Geschwindigkeit von 10 Gbps Angriffe in Echtzeit ab und ist die einzige von der NSS Group zertifizierte IPS-Lösung.

McAfee UTM Firewall ist die kostengünstige Lösung zur Authentifizierung von Remote-Anlagen und zur Sicherung von drahtlosen Kommunikationswegen.

McAfee Network Access Control Module setzt die Richtlinienkonformität durch und stellt sicher, dass Konfigurationen der Sicherheitssysteme auf den Geräten von Mitarbeitern, Auftragnehmern und anderen Anbietern aktuell sind.

McAfee Network User Behavior Analysis ermöglicht über einen eigenen Datenweg (out-of-band) Echtzeit-Überwachung des tatsächlichen Verhaltens namentlich identifizierter Anwender, um punktgenau festzuhalten, welche Person an welchem Ort und zu welchem Zeitpunkt etwas tut.

McAfee Network DLP Manager erkennt und versteht Ihre Daten und ordnet sie gemäß Ihren Sicherheitsrichtlinien Sicherheitsstufen zu.

McAfee Email Gateway beseitigt nicht nur Spam und Mails mit Malware, sondern schützt zugleich automatisch vor Datendiebstahl – und das alles in einer einfach zu verwaltenden Appliance.

McAfee Web Gateway bietet mit einer Filtergenauigkeit von 99,94 Prozent und einer False-Positive-Quote von 0,02 Prozent lückenlosen Schutz vor Malware, die sich über das Internet verbreitet.

McAfee Network Access Control Module

McAfee Network Access Control Module bietet identitätsbasierte Zugriffssteuerung zur Erfüllung der Anforderungen kritischer Netzwerke. Anstatt nur den Zugriff auf das Netzwerk für riskante Systeme zu sperren, können Sie Richtlinienkonformität durchsetzen, um sicherzustellen, dass Anwender keine Sicherheits-Tools deaktivieren, schädliche Anwendungen installieren oder Sicherheitseinstellungen verwalten lassen.

McAfee Network User Behavior Analysis

McAfee Network User Behavior Analysis (Securify) bietet einzigartige Identitätsüberwachungs- und Blockierfunktionen zum Schutz des Unternehmens vor Bedrohungen von innen. Wie der Name bereits andeutet, stellt es mithilfe einer Analyse des Anwenderverhaltens identitätsabhängige, netzwerkbasierte Strategien bereit, mit denen bestehende Infrastrukturen genutzt werden, um über umfangreiche Netzwerke und Systeme hinweg kostengünstig konkrete Zugriffe zu erkennen und zu steuern sowie das allgemeine Verhalten der Anwender zu kontrollieren. McAfee Network User Behavior Analysis bietet folgenden Möglichkeiten:

- Erkennung von Netzwerk- und Service-Scans, die beide Vorbereitungsmaßnahmen für gezielte Angriffe sein können
- Sofortige Erkennung von nicht autorisierten Quellen und Anwendern, die Zugang zu kritischen Unternehmenssystemen erhalten
- Erkennung von Anzeichen kompromittierter oder manipulierter Ressourcen wie IRC-Steuerkanäle oder Zugriffe über Backdoors
- Überprüfung auf berechtigten Zugriff mit der Möglichkeit, Transaktionen mit tatsächlichen und namentlich aufgeführten Anwender-Identitäten in Bezug zu setzen
- Kontrolle der autorisierten Verwendung mit Grenzwerten für die erwarteten Mengen übertragener Daten zur Vorbeugung gegen das Herausschleusen kritischer Daten
- Erkennung von unzulässiger Verwendung (selbst wenn Anmeldedaten über Social Engineering erschlichen wurden) unter anderem anhand von zu hoher Zahl an Anmeldungen, ungewöhnlichen Mengen von Datenverkehr und Zugriffen von unerwarteten oder nicht zugelassenen Standorten, wie Remote-Netzwerken aus
- Erkennung und Verhinderung von Missbrauchsversuchen wie unerwartete Öffnung von ausgehenden Verbindungen oder Tunneln für Kommunikation und Datenübertragung

McAfee Network DLP Manager

Mit McAfee Network DLP Manager können Sie gespeicherte, in Verwendung oder in der Übertragung befindliche vertrauliche Daten schnell und einfach identifizieren und schützen. Es bietet zentrale Verwaltung, Auditierung, Reporting, Zwischenfall- und Fallverwaltung sowie eine detaillierte Forensik in Kombination mit innovativen Lernfunktionen und senkt so den Zeit- und Arbeitsaufwand für die Einrichtung eines Schutzsystems erheblich. McAfee Network DLP Manager kann die Betriebskosten erheblich senken und Unternehmen in die Lage versetzen, sich schnell an im Wandel befindliche geschäftliche Anforderungen anzupassen.

McAfee Email Gateway

Wesentlicher Bestandteil einer vollständigen „Defense in Depth“-Strategie ist der Schutz des E-Mail- und Web-Datenverkehrs. McAfee Email Gateway (ehemals IronMail) ist die führende E-Mail-Sicherheits-Appliance auf dem Markt und bietet ein lückenloses Sortiment bidirektionaler Sicherheitstechnologien zum Schutz ein- und ausgehender E-Mails. So ist für den Schutz von E-Mails, die Durchsetzung von Richtlinien und die Verschlüsselung vertraulicher Daten gesorgt – und dies mit einer Filtergenauigkeit von 99 Prozent und nur 0,001 Prozent False-Positives. Mithilfe des weltweit über TrustedSource ermittelten Wissens ist Spam kein Thema mehr, und Verschlüsselungs- sowie Datenschutzrichtlinien werden automatisch durchgesetzt.

McAfee Web Gateway

McAfee Web Gateway (ehemals Webwasher) ist eine Sicherheits-Appliance, die zwischen interne Arbeitsplatzrechner und die von dort aus aufgerufenen Webseiten geschaltet ist. McAfee Web Gateway-Appliances verhindern nicht nur den Zugriff von Mitarbeitern auf nicht geschäftsbezogene oder unangemessene Webseiten, sondern schützen vor allem Desktop-Rechner vor einer Kompromittierung oder Infektion über den von den Mitarbeitern verwendeten Browser, und zwar auch auf verschlüsselten Webseiten. Mit McAfee Web Gateway müssen sich IT-Administratoren keine Sorgen machen, dass Desktop-Rechner in ferngesteuerte Zombies verwandelt werden, sich mit Spyware infizieren oder durch Malware beschädigt werden. Vor allem müssen sie auch nicht länger fürchten, dass von kontaminierten Desktop-Rechnern aus Infektionen auf kritische Netzwerke überspringen könnten.

Kombinierter Schutz

Die Technologien von McAfee ergänzen sich gegenseitig und schützen Steuersysteme. McAfee Network DLP Manager, McAfee Email Gateway und McAfee Web Gateway bieten Schutz vor Datendiebstahl aus dem Unternehmensnetzwerk heraus, um so Daten auf kritischen Anlagen zu schützen. McAfee UTM Firewall und McAfee Network Access Control Module schützen Remote-Standorte durch Geräte-Authentifizierung und die Überprüfung der Richtlinienkonformität. McAfee Network User Behavior Analysis sorgt für eine interne Anwenderüberwachung und hilft dabei, verdächtige Verhaltensweisen zu unterbinden. McAfee Firewall Enterprise und McAfee Network IPS Manager schließlich schützen die Peripherie der Steuerzentrale vor Angriffen von jedem möglichen Zugangspunkt aus. Darüber hinaus gewährleisten die umfassenden Reporting-Funktionen die Einhaltung von unternehmensinternen Richtlinien und staatlichen Vorschriften.

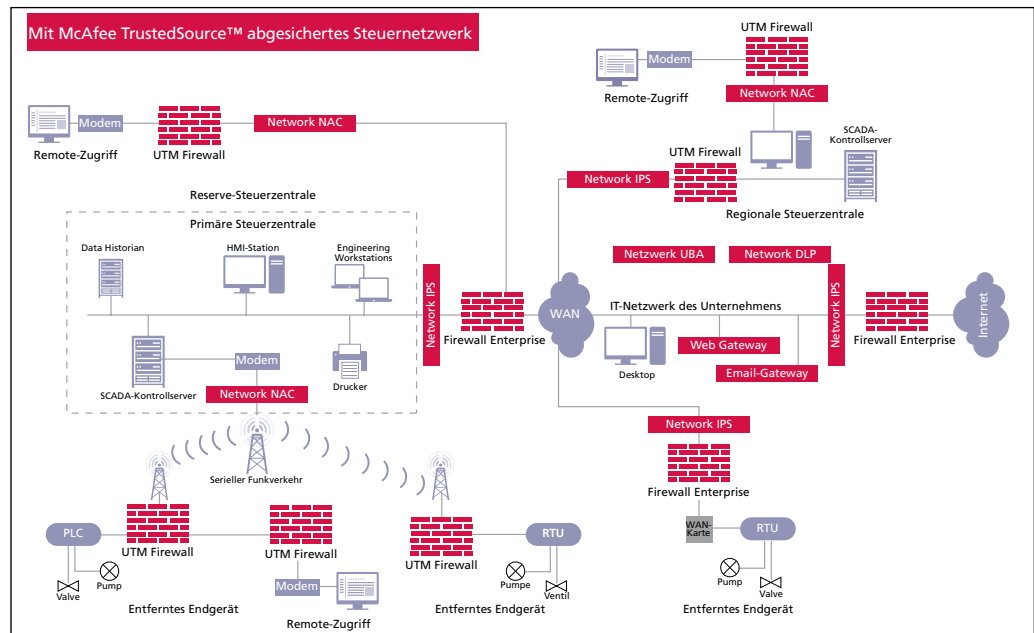


Abbildung 6: Schutz einer Steuerzentrale mit Lösungen von McAfee.

Zusammenfassung

Bedrohungen für kritische Infrastrukturen nehmen Jahr für Jahr sowohl zahlenmäßig als auch an Raffinesse zu. Schlimmer noch ist, dass diese Bedrohungen sich in dem Maße, wie Hacker immer bessere Kenntnisse erlangen und auf neue Technologien zurückgreifen können, weiterhin vermehren und an Gefahrenpotenzial zunehmen werden. Da Angriffe, die bei IT-Netzwerken an der Tagesordnung sind, nun zunehmend auch Steuernetze infiltrieren, ist ein zuverlässiger Schutz unverzichtbar. Dieser darf jedoch nicht die Verfügbarkeit, Integrität und Zuverlässigkeit des Steuernetzes beeinträchtigen.

Eigentümer kritischer Infrastrukturen sollten die Umsetzung jeder der nachstehend aufgeführten, als „Best Practice“ empfohlenen Sicherheitsmaßnahmen erwägen, um ihre kritischen Netzwerke, ihre Investitionen und ihre Kunden zu schützen:

1. Ausbringung von Echtzeitschutz
2. Abtrennung und Abschirmung kritischer Infrastrukturen von verbundenen Netzwerken
3. Kontrolle der Zugriffsberechtigungen und der Netzwerkaktivitäten
4. Schutz von Daten über kritische Infrastrukturen vor Diebstahl
5. Ausbringung eines zuverlässigen Schutzes ohne Beeinträchtigung von Verfügbarkeit, Integrität und Zuverlässigkeit

Der richtige Sicherheitspartner für Sie ist derjenige, der sich voll und ganz auf Sicherheit konzentriert und Ihnen langfristig zur Seite steht. McAfee hat mehr als 15 Jahre Erfahrung in der Ausbringung von Lösungen für kritische Infrastrukturen in Stromerzeugungseinrichtungen, bei Regierungsstellen und Transportbehörden, in der Wasser-, Strom- und Gasversorgung sowie bei petrochemischen und chemischen Betrieben in 28 US-Bundesstaaten und 5 kanadischen Provinzen sowie in den Ländern Großbritannien, den Jungferninseln, Italien, Deutschland, Hongkong, Japan, Australien, Polen, Österreich, Thailand, Neuseeland, Oman, Brunei, Saudi-Arabien, Irland, Kuwait, Brasilien, Malaysia, Qatar, Pakistan, Südafrika, Taiwan, den Philippinen, Finnland und Dänemark.

McAfee hat Lösungen für kritische Infrastrukturen in Stromerzeugungseinrichtungen, bei Regierungsstellen und Transportbehörden, in der Wasser-, Strom- und Gasversorgung sowie bei petrochemischen und chemischen Betrieben geliefert. Unser umfassendes Sortiment an Netzwerksicherheitslösungen stellt die Erfüllung der drei wichtigsten Kriterien sicher, nach denen Administratoren kritischer Infrastrukturnetze sich heutzutage richten müssen:

- Schutz der Netzwerke, ohne dass die Einhaltung wichtiger Verfügbarkeitsvorgaben gefährdet ist
- Einhaltung von unternehmensinternen, branchenweit sowie auf regionaler, nationaler und internationaler Ebene geltenden Vorschriften
- Einhaltung von Finanzvorgaben

Allerdings sind die besten Produkte der Welt nutzlos, wenn sie nicht durch Weltklasse-Support unterstützt werden. Falls es jemals zu einem Vorfall kommt, sind die meisten McAfee-Kunden in Minutenschnelle mit einem qualifizierten Mitarbeiter verbunden.

McAfee kann Sie in einer immer stärker vernetzten und damit auch immer gefährlicheren Welt dabei unterstützen, die fünf wesentlichen Möglichkeiten zum Schutz Ihrer kritischen Netzwerke umzusetzen. Weitere Informationen erhalten Sie unter www.mcafee.com/de oder unter der Telefonnummer +49 (0)89 3707 0.

Informationen zu McAfee

McAfee (NYSE: MFE) ist einer der weltweit größten dedizierten Spezialisten für IT-Sicherheit. Das Unternehmen mit Hauptsitz im kalifornischen Santa Clara hat sich der Beantwortung anspruchsvollster Sicherheitsherausforderungen verschrieben. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer und ITK-Netze auf der ganzen Welt vor Angriffen schützen und es Anwendern ermöglichen, gefahrlos Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Dank seines preisgekrönten Forschungsteams entwickelt McAfee innovative Produkte, die es Privatanwendern, Unternehmen, dem öffentlichen Sektor und Service-Providern ermöglichen, gesetzliche Vorschriften einzuhalten, Daten zu schützen, Ausfälle zu vermeiden, Schwachstellen zu erkennen und ihre Sicherheit fortlaufend zu überwachen und zu verbessern. www.mcafee.com/de.

McAfee GmbH
Ohmstraße 1
85716 Unterschleißheim
Deutschland
Telefon: +49 (0)89 3707 0
www.mcafee.com/de

