

1 Relevanz von Netzwerken in KMUs

Computernetzwerke sind innerhalb von Unternehmen und Institutionen ein notwendiger, unabdingbarer Teil der Infrastruktur geworden und werden oftmals für die Übertragung vertraulicher Informationen genutzt. Das Spektrum reicht hierbei von Emails über Telefonie bis hin zur Übertragung von unternehmenskritischen Daten, die für Dritte einen Wettbewerbsvorteil bedeuten können (Industriespionage).

Ein erfolgreicher Angriff und der damit verbundene Verlust der Vertraulichkeit können schwere finanzielle Schäden als auch, wenn es sich um personenbezogene Daten handelt, eine Verletzung des Datenschutzes mit allen Konsequenzen zur Folge haben. Das Risiko eines solchen Vorfalls kann nur dann dauerhaft gering gehalten werden, wenn die beteiligten Applikationsprogramme und die verwendeten Rechner als auch die Kommunikationswege "sicher" (durch kryptographische Verfahren geschützt) sind, und die Struktur des zugrundeliegenden Netzwerks möglichst wenige Angriffspunkte offenbart und durch den Einsatz intelligenter Systeme in der Lage ist, Angriffe zu erkennen. Die Notwendigkeit solcher Schutzmaßnahmen wird insbesondere dann deutlich, wenn neben kabelgebundenen Komponenten auch drahtlos kommunizierende Komponenten zum Einsatz kommen. Aufgrund der besonderen Exposition der Luftschnittstelle gegenüber aktiven Angriffen bzw. passivem Abhören bedürfen gerade diese Art Netzwerke besonderen Schutzes.

1.1 Analyse des bestehenden Netzwerks

Der vom DETOS Projekt verfolgte Ansatz basiert auf mehreren Schritten zur erfolgreichen Absicherung eines Unternehmensnetzwerks. Der erste Schritt ist hierbei die Analyse des Netzwerks mit geeigneten Methoden. Hierzu wird eine Analyseeinheit zu Beginn der Analysephase für einen bestimmten Zeitraum in das vorhandene Netzwerk eingebracht, um Informationen über die einzelnen Komponenten und deren Kommunikationsverhalten zu sammeln.

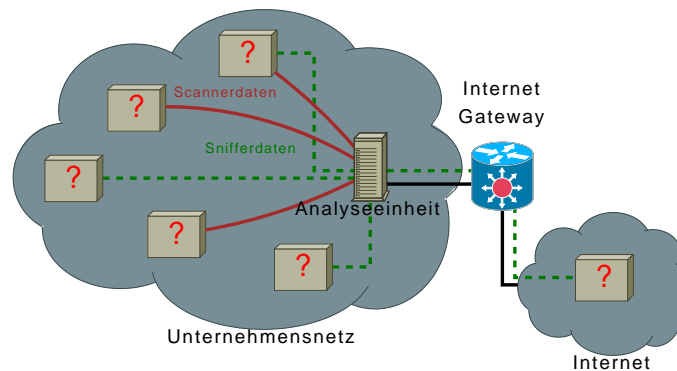


Abbildung 1: Analyse des Unternehmensnetzkes

Abbildung 1.1 zeigt die Besonderheit des hierbei eingesetzten hybriden Verfahrens: Zum einen wird das Netzwerk passiv beobachtet, was später eine Analyse des Kommunikationsverhaltens der Applikationen bzw. Komponenten untereinander ermöglicht. Die aus der Analyse resultierenden Informationen sind nötig, um beispielsweise (verschlüsselten) Verkehr zu Mailservern oder die Nutzung von Instant Messaging Programmen zu erkennen. Zum anderen werden die Komponenten aktiv auf Schwachstellen hin untersucht. Dieser Teil wird durch Portscans und Penetration Tests zu unterschiedlichen Zeitpunkten in der Analysephase realisiert. Die auf diese Art gewonnenen Daten lassen eine sehr viel feinere Schutzbedarfsanalyse zu, da nicht nur ein einmaliger Blick auf das Netzwerk, sondern die ständige Überwachung über einen bestimmten Zeitraum eine sehr viel größere Datenbasis bereitstellt. Das wiederum ermöglicht individuellere, auf das jeweilige Netzwerk zugeschnittene Analyseergebnisse (Abbildung 1.1).

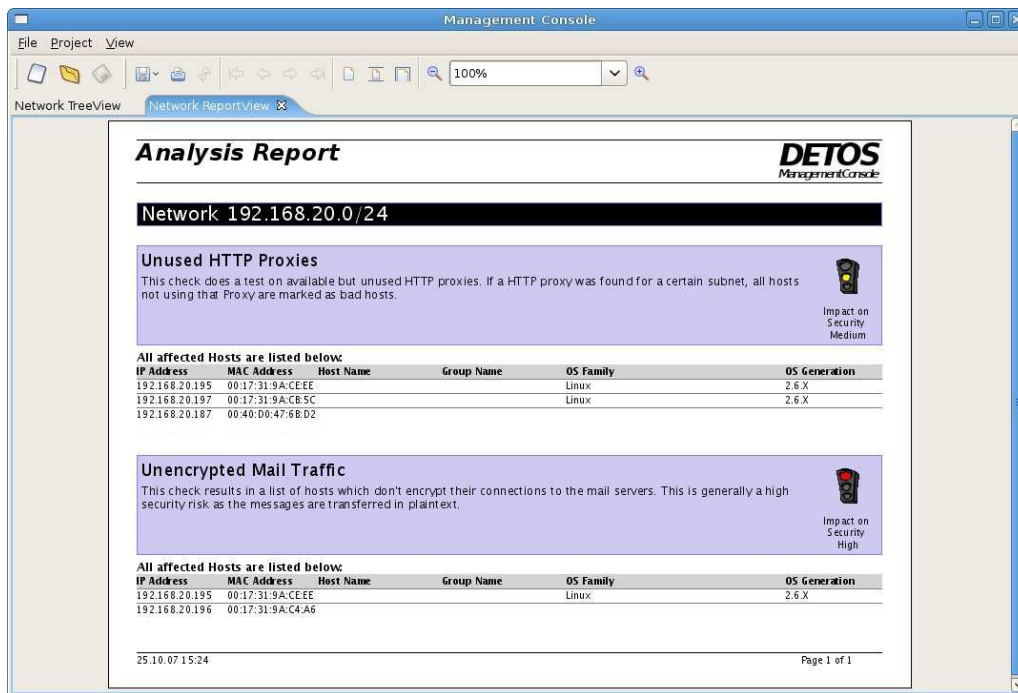


Abbildung 2: Report der Sicherheitsanalyse nach Auswertung der gesammelten Daten

Um sicherzustellen, dass der Datenschutz während der Analysephase gewährleistet ist, werden keinerlei Nutzdaten aufgezeichnet. Lediglich Informationen über die Kommunikationspartner (die Adressen der Quelle und des Ziels) und die Art des Verkehrs werden zur späteren Analyse gespeichert. Hierin liegt letztendlich ein weiterer Vorteil des Verfahrens: Die zu bewältigende Datenmenge aus der Analysephase wird gering gehalten, was bei der Aufzeichnung der Daten weniger Ressourcen benötigt und sich bei der anschließenden Verarbeitung der Daten mit einer geringen Dauer bemerkbar macht.

1.2 Umstrukturierung des Netzwerks sowie Absicherung und Kontrolle der Kommunikationswege

Im folgenden zweiten Schritt nach Abschluss der Analysephase wird die Analyseeinheit aus dem Netzwerk entfernt, und die gewonnene Daten werden von einer Applikation (Managementkonsole) ausgewertet (Abbildung 1.2). Anschließend erfolgt eine programmgestützte und individualisierte Befragung (Fragebogen) des zuständigen IT-Betreibers (Anwender) im Unternehmen. Zum einen wird hierbei festgestellt, ob die ermittelten Daten vollständig sind oder ob noch weitere Dinge berücksichtigt werden müssen, welche dann wiederum vom Anwender manuell spezifiziert werden können. Zum anderen bekommt der Anwender jetzt die Möglichkeit festzulegen, welche Kommunikationswege nach der automatisierten Umstrukturierung und Absicherung des Netzwerks genutzt und welche nicht genutzt werden können. Diese Aufgabe wird insofern stark vereinfacht, als dass die Applikation Sicherheitsmängel im Netzwerk automatisch erkennt und Lösungsvorschläge präsentiert.

Besonderheit hierbei ist die Möglichkeit für den Anwender, aus vorgefertigten Modulen für häufige Anwendungsfälle in KMUs auswählen zu können. Das ermöglicht eine individuelle Anpassung an die Gegebenheiten im Unternehmen (Abbildung 1.2). Die bisherige Planung umfasst die Basismodule Routing und Firewalling, HTTP Proxyserver und automatisierte Sicherheitschecks. Diese Module werden als Minimum automatisch installiert und gewährleisten somit einen rudimentären Schutz gegen Angriffe. Weitere geplante Module für mehr Sicherheit umfassen die Bereitstellung einer lokalen Certificate Authority, die Schaffung einheitlichen Authentifizierungsinfrastruktur auf

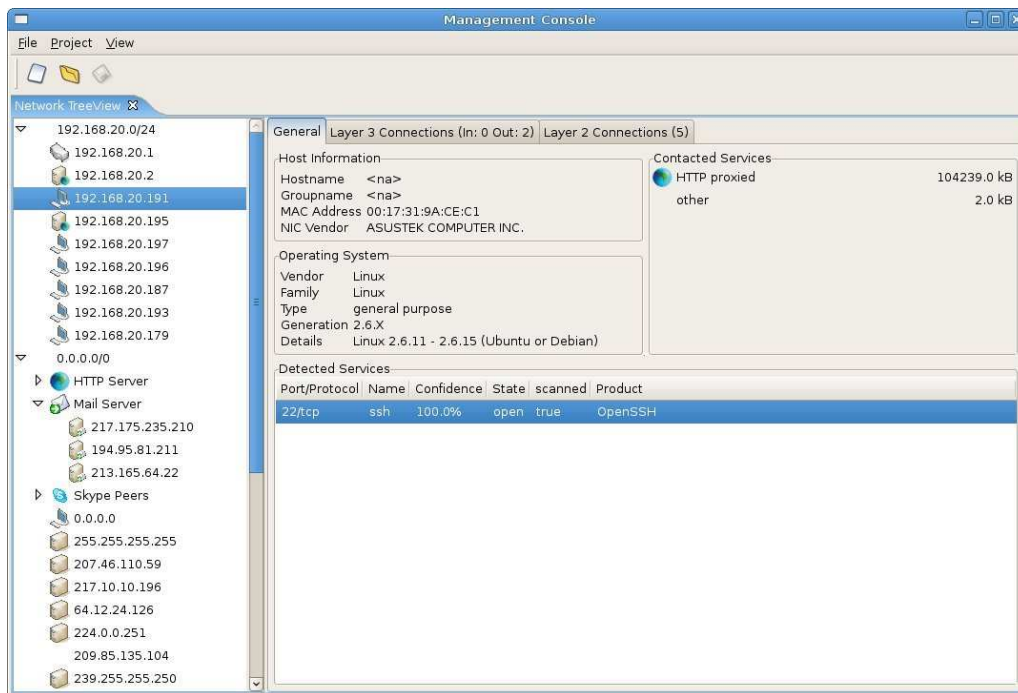


Abbildung 3: Ausgewertete Analysedaten einer Arbeitsstation in der Managementkonsole

Basis von Radius und LDAP, die Anbindung von Zweigstellen oder Außendienstmitarbeitern mittels VPN, Authentifizierung im WLAN mittels IEEE 802.1X und Radius-Backend, Bereitstellung eines Mailservers mit Spam- und Malwarefilter sowie Intrusion Detection/Prevention Systeme.

Das folgende Beispiel verdeutlicht das weitere Vorgehen nach Abschluss der Analysephase. Die Auswertung der gesammelten Daten hat ergeben, dass alle Rechner im Netzwerk ihre Mails bei einer Maschine M im eigenen Netz abholen. Maschine M dient als interner Mailserver, zeigt bei weiterer Beobachtung jedoch zusätzlich ein Verhalten, das typischerweise auf einen Arbeitsplatzrechner hindeutet. Aus diesem Grund kann M nicht eindeutig klassifiziert werden und fällt somit in beide Klassen "Arbeitsplatzrechner" als auch "(Mail)server". Eine Richtlinie der Analyseapplikation legt fest, dass Maschinen, die offensichtlich als Server auftreten, in einem besonders geschützten Bereich des Netzwerks platziert werden müssen. Die Verletzung dieser Richtlinie veranlasst die Applikation dem Anwender den Vorschlag zu unterbreiten, den als Mailserver genutzten Arbeitsplatzrechner physikalisch auf zwei Maschinen aufzuteilen und den neu entstandenen Server in einem separaten Netzsegment unterzubringen. Optional dazu wird dem Anwender noch die Installation des Moduls "Mail" offeriert, welches einen eigenen Mailserver für den Einsatz im Unternehmen mit Spam- und Malwarefilter mitbringt.

Das von der Applikation auf Basis der Analysedaten angefertigte Konzept zur Umstrukturierung muss im nächsten Schritt umgesetzt werden. Sofern physikalische Änderungen vorgenommen werden müssen, erstellt die Applikation einen detaillierten Plan, der den Anwender bei den anfallenden Arbeiten unterstützen soll. Diese Anleitung ist leicht verständlich gehalten und wird durch Schaubilder verdeutlicht. Im Laufe der physikalischen Umstrukturierung werden auch eine oder mehrere neue Komponenten im Netzwerk eingefügt. Diese neuen Komponenten sind Bestandteile der DETOS Plattform und haben unter anderem zur Aufgabe, den Verkehr an bestimmten Stellen im Netzwerk mit geeigneten Mitteln wie z.B. Paketfilter-Firewalls oder Proxy-Servern dem erarbeiteten Konzept entsprechend zu kontrollieren und regulieren. Weitere Komponenten wie der im obigen Beispiel genannte Mailserver werden in dieser Phase ebenfalls im Netzwerk integriert.

Die Besonderheit dieses Ansatzes ist auch hier die weitestgehend automatisierte Installation und Konfiguration der benötigten Komponenten und Module von der Managementkonsole aus. Die einzigen vom Anwender zu leistenden Arbeiten sind die Bearbeitung des Fragebogens und die Mod-

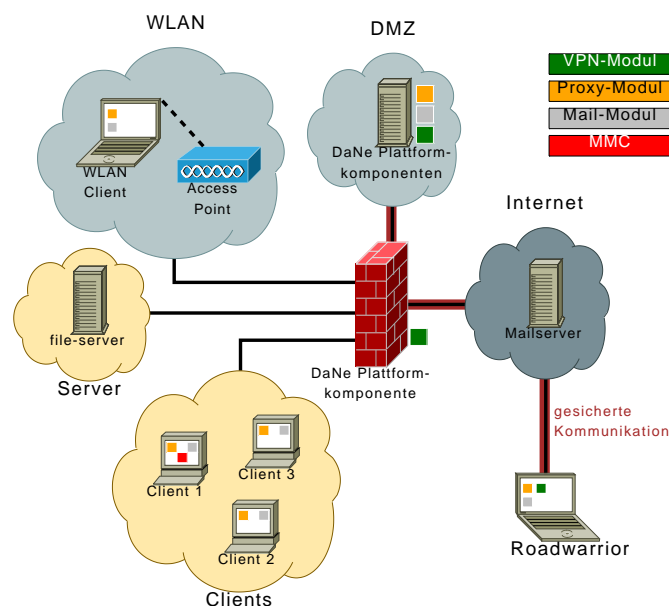


Abbildung 4: Restrukturiertes Netzwerk mit Modulen für VPN, Proxy und Mail

ulassung sowie alle nicht automatisierbaren Vorgänge wie die physikalische Umstrukturierung des Netzwerks und die Installation der Plattform auf den benötigten Komponenten. Letzteres beschränkt sich im Endstadium jedoch auf das Einlegen einer CD oder DVD in ein entsprechendes Laufwerk der neu zu installierenden Maschine und das anschließende Booten vom eingelegten Medium aus. Die Installation läuft auf Wunsch vollautomatisch ab, und nach Abschluss der Installation sowie dem Anschluss an das Netzwerk wird das Gerät von der Managementkonsole erkannt und nach Rückfrage an den Anwender entsprechend dem Konzept konfiguriert.

1.3 Überwachung des Netzwerks und Reporting

Während der Umstrukturierungsphase wurden die neuen Komponenten der DETOS Plattform im Netzwerk eingebracht und die aktuell vorhandenen Sicherheitsmängel behoben. Der dritte Schritt zur erfolgreichen Absicherung eines Netzwerks besteht in der Überwachung des Netzes im laufenden Betrieb.

Hierzu werden folgende Maßnahmen getroffen:

- Alle Maschinen im Netzwerk werden auf die Aktualität der Software hin überwacht. Veraltete Software stellt oftmals ein Sicherheitsrisiko dar und muss deshalb vermieden werden. Mittlerweile bieten die meisten Hersteller von Betriebssystemen zu bekanntgewordenen Sicherheitslücken relativ zeitnah Patches an. Diese müssen schnellstmöglich installiert werden, damit die Sicherheitslücken nicht zu einem Risiko für das Netzwerk werden.
- Die Aktualität als auch die Aktivität der Antivirensoftware werden überwacht. Ein ungeschützter Rechner stellt nicht nur ein Sicherheitsrisiko für die auf ihm enthaltenen Daten dar, sondern für das gesamte Netz mit allen seinen Komponenten. Ist ein Rechner erst einmal mit Malware befallen bestehen für deren Ausbreitung im Intranet nun weitaus bessere Möglichkeiten. Angefangen von Viren, die Daten auf einem Fileserver zerstören über Würmer, welche die Daten ausspähen und an Dritte verschicken bis hin zum schlimmsten Fall, dass z.B. durch einen Trojaner ein externer Angreifer direkten Zugriff auf den Rechner erlangt hat und jetzt als "interner" Angreifer gezielt sensible Daten im Netzwerk ausspionieren oder ganz und gar die Kontrolle über andere Maschinen erlangen kann.
- Der optionale Einsatz eines Intrusion Detection/Prevention Systems (IDS/IPS) ermöglicht die

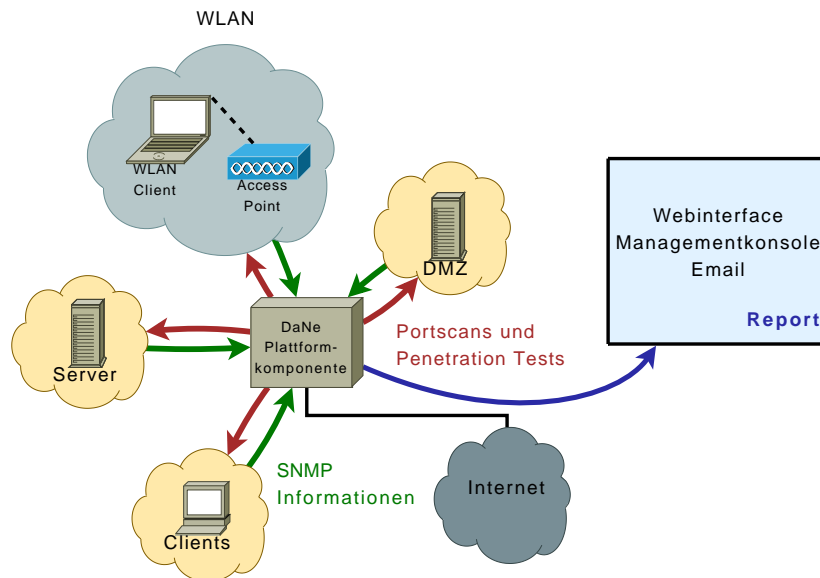


Abbildung 5: Überwachung des Netzwerks und seiner Komponenten

Entdeckung von Angriffen während diese geschehen, so dass der zuständige IT-Beauftragte zeitnah informiert werden kann und/oder der Angriff ganz und gar durch Eingreifen des IPS vereitelt werden kann. Ein IDS hilft natürlich nicht immer, den Angriff rechtzeitig zu stoppen, doch liefert es einen wertvollen Beitrag zur Klärung der Frage, welche Daten/Maschinen wurden kompromittiert und wer hat bzw. von wo aus wurde der Angriff durchgeführt. Der Einsatz eines IDS oder IPS ist jedoch mit enormen Kosten für die Anschaffung der benötigten Hardware und Schaffung einer geeigneten Infrastruktur verbunden. Das ist gerade in kleinen Unternehmen eine kaum zu überwindende Hürde, weshalb diese Schutzmaßnahme auch nur als Modul verwirklicht wird und kein Kernbestandteil unserer Lösung ist.

- Als letzte Maßnahme werden in bestimmten Intervallen Portscans und Penetrationstests durchgeführt. Diese Aktionen sollen von Virenscannern eventuell nicht bemerkte, unerwünscht laufende Dienste aufdecken und die durch nicht eingespielte Sicherheitspatches entstandenen Sicherheitslücken offenlegen.

Die technische Realisierung der ersten beiden Maßnahmen basiert zum einen auf der zentralen Überwachung der Komponenten mittels SNMP von Seiten einer Komponente der DETOS Plattform. Alle nicht über SNMP verfügbaren Informationen werden durch ein plattformunabhängiges Java-Programm ermittelt und an die zentrale Stelle übertragen. Diesen Informationen werden mit den gesammelten Daten aus den IDS/IPS Logs sowie mit dem aus den Portscans und Penetrationstests gewonnenen Wissen kombiniert und in einem wöchentlichen Bericht für den IT-Beauftragten leicht verständlich zusammengefasst.