

Link: <https://www.tecchannel.de/a/sicherheitsluecke-roadwarrior,402189>

Konzepte zur Absicherung mobiler Clients Sicherheitslücke Roadwarrior

Datum: 16.05.2008
Autor(en): Mike Hartmann

Mit Notebook, PDA oder Smartphone kann der Roadwarrior seiner Tätigkeit überall nachgehen. Doch wer beim Einsatz mobiler Geräte nicht aufpasst, riskiert damit nicht nur die Sicherheit seines LAN.

Anstatt USB-Sticks zwischen Büro und Heimbüro hin und her zu tragen, hat der Manager von heute die relevanten Dateien immer auf seinem Laptop dabei. Beim Kunden schnell eine Präsentation halten? Kein Problem. Abends noch mal kurz Emails lesen oder die letzten Änderungen an den Verkaufsprognosen und Marketing-Strategien machen, die Zeit im Flugzeug produktiv nutzen und dann in der Firma gleich die neuesten Infos für die Mitarbeiter im Netz ablegen. Auch das ist mit einem Notebook und einer Internet-Verbindung problemlos realisierbar.

Das Netzwerk ist natürlich gegen Angriffe von außen mit einer Firewall ausgestattet, und Verbindungen ins LAN werden nur über VPN oder SSH realisiert. Andere Server, die von außen erreichbar sein müssen, stehen in der DMZ und sind entsprechend abgeschottet. Der Email-Server ist mit Virens Scanner, Content-Filter und Spam-Schutz ausgestattet, und der Webzugriff vom LAN ins Internet erfolgt über einen Proxy, der ebenfalls den Datenverkehr auf schädlichen Code untersucht. Dass interne Server mit einem On-Access-Virens Scanner ausgestattet sind und alle Virens Scanner ständig über die aktuellsten Signaturen verfügen, versteht sich von selbst.

Insgesamt also ein ausgeklügeltes, mehrstufiges Sicherheitssystem. Und dennoch kann sich ein Wurm wie der Blaster ungehindert in eine solche "Bastion" einschleichen? Ja, denn in sehr vielen Netzwerken gilt der (ungeschriebene) Grundsatz: "Wer drin ist, dem vertrauen wir!"

Genauso brauchen sich Wirtschaftsspione auch nicht unbedingt die Mühe machen, sich durch die vielstufigen Verteidigungsanlagen zu kämpfen, wenn die Daten ohnehin auf Laptop, Smartphone oder USB-Stick das Haus verlassen.

1. Notebook als Einfallstor

Solange das Notebook also nur im lokalen Netz betrieben wird, ist es durch die Sicherheitsmechanismen des LAN geschützt. Für den mobilen Mitarbeiter besteht jedoch ein Großteil der Vorteile darin, dass er das Notebook auch zu Hause oder unterwegs einsetzen kann. Und sobald er es zu Hause per DSL, im Hotel per DFÜ-Netzwerk oder anderswo per WLAN-Hotspot oder UMTS-Handy mit dem Internet verbindet, ist es vorbei mit der Sorglosigkeit. Ohne aktuelle Sicherheits-Patches würde er sich beispielsweise schnell ohne eigenes Zutun einen **Blaster-Wurm**¹ einfangen oder beim normalen Surfen mit dem Internet Explorer dank diverser Sicherheitslücken andere Viren, Trojaner oder Würmer.

Kommt er dann vom Außeneinsatz zurück und hängt das Notebook in die Dockingstation, steht dem Schadcode das gesamte LAN mehr oder minder ungeschützt offen. Der Blaster könnte alle ungepatchten Windows-Rechner befallen, weil die schützende Firewall fehlt. Server wären durch den Virenschanner eventuell noch vor Viren geschützt, aber Clients mit irgendwelchen lokalen Freigaben nicht.

Wenn Sie also Mitarbeiter mit einem Firmen-Notebook in die "freie Wildbahn" lassen wollen, sind einige Sicherheitsvorkehrungen unabdingbar.

2. Sicherheitsvorkehrungen am Notebook

Optimal wären natürlich zwei verschiedene Installationen von Windows auf verschiedenen Partitionen, die jeweils voreinander versteckt sind. Damit ist das für den Einsatz im LAN vorgesehene Windows komplett abgeschottet, wenn der Benutzer unterwegs arbeitet. Mit einem Boot-Manager stellt das auch kein großes Problem dar. Allerdings ist dann der Datenaustausch zwischen den beiden Partitionen nicht möglich. Um also das Szenario "Präsentation aus der Firma mitnehmen und zu Hause bearbeiten" realisieren zu können, sind zusätzliche Maßnahmen erforderlich. Etwa der Datenaustausch über Email oder ähnliche Verfahren.

Allerdings vervielfachen sich bei dieser Lösung die Probleme, etwa mit verschiedenen, konkurrierenden Dateiversionen. Wenn Sie daher auf den direkten Austausch von Dateien nicht verzichten wollen und deshalb die Benutzer nicht mit getrennten Partitionen arbeiten lassen, sollten Sie unbedingt das mobile Gerät absichern und auch im LAN entsprechende Vorkehrungen treffen.

Die wichtigste Maßnahme besteht darin, dass die aktuellsten Sicherheits-Patches für Windows und den Internet Explorer eingespielt werden sollten. Und zwar am besten, ohne dass der Benutzer eingreifen muss oder darf. Wenn Sie den **Software Update Service im LAN**² einrichten, müssen Sie sich nicht mehr darauf verlassen, dass die Benutzer regelmäßig bei **Windows Update**³ vorbeischaun. Zudem behalten Sie die Kontrolle über die installierten Patches und müssen sich keine Gedanken darüber machen, ob Windows Update irgendwelche Daten an Microsoft überträgt.

3. Weitere Maßnahmen

Der lokale Benutzer des Notebooks sollte nicht als Hauptbenutzer eingetragen sein. Für den Internet Explorer richten Sie die erlaubten ActiveX-Controls wie beispielsweise Flash oder Netmeeting vorab ein und sperren dann den Download weiterer Controls per Group Policy Editor (gpedit.msc).

Als weitere Sicherheitsmaßnahmen sollten Sie die Sicherheitszonen und -einstellungen optimieren, so dass dem Browser per Default nur wenig erlaubt ist. Natürlich müssen Sie dem Benutzer die Möglichkeit entziehen, selbst Änderungen an den Sicherheitseinstellungen vorzunehmen. Auch diese Konfiguration können Sie beim **Active Directory**⁴ per Policy automatisch an die Benutzer verteilen lassen.

Mit Tools wie **Spybot Search&Destroy**⁵ können Sie den IE weiter absichern. Die Funktion "Immunisieren" sperrt beispielsweise als gefährlich erkannte ActiveX-Controls. Und über die Hosts-Datei können Sie den Zugriff auf potenziell gefährliche oder unerwünschte Websites verhindern.

Des Weiteren ist der Einsatz eines Virenschanners auf dem Notebook unabdingbar. Zwar sollte ein solcher Scanner auf allen Rechnern im LAN laufen, aber bei mobil eingesetzten Geräten ist ein Verzicht geradezu grob fahrlässig. Zu einem Virenschanner gehören immer auch aktuellste Signaturen, damit er überhaupt Sinn macht. Eine zentral verwaltete Antivirus-Lösung ist auch hier besser, als es dem einzelnen Benutzer zu überlassen, sich mit aktuellen Signaturen zu versorgen.

4. Dienste abschalten

Per Default wird bei Windows eine ganze Reihe von Diensten gestartet, die teilweise überflüssig sind und teilweise sogar die Sicherheit gefährden, wenn sie auf einem Rechner laufen, der ungeschützt mit dem Internet verbunden ist.

So sollten beispielsweise der Nachrichtendienst, der Server-Dienst und Remote Registry außerhalb des LAN abgeschaltet sein. Auch andere Windows-Services, die den entfernten Zugang zu Verwaltungsfunktionen des Rechners erlauben, sollten Sie abschalten oder deaktivieren. Für Windows XP bietet unser Beitrag **XP-Dienste aufräumen**⁶ eine Liste der nicht benötigten Funktionen. Entsprechend hilft Ihnen unser Beitrag **Vista-Dienste aufräumen**⁷ bei der Absicherung von Systemen unter Windows Vista.

Wird das Notebook innerhalb des LAN eingesetzt, machen diese Dienste allerdings durchaus Sinn. Denn Sie als Administrator wollen ja durchaus die eingesetzten Geräte verwalten - und zwar von einer zentralen Station aus und nicht, indem Sie zu jedem Rechner laufen.

Hier haben Sie zwei Möglichkeiten:

Erstellen Sie mehrere Profile, die der Anwender dann je nach Ort beim Rechnerstart auswählt. Dies ist allerdings insoweit fehleranfällig, als dass Sie sich dabei auf den Benutzer verlassen müssen. Zudem ist diese Variante unter Vista nicht verfügbar.

Erstellen Sie im LAN ein Anmelde-Script, das die benötigten Dienste nachstartet. Dazu benutzen Sie den Kommandozeilen-Befehl

```
net start dienstname
```

. Der Beitrag zu Diensten unter Windows Vista beschreibt die **Besonderheiten einer Batch-gesteuerten Dienste-Abschaltung**⁸.

5. Lokale Firewall

Über Sinn und Unsinn von **Personal Firewalls**⁹, auch Desktop Firewalls genannt, im Firmennetz wird immer wieder heftig debattiert. Für mobile Benutzer, die in Hotels oder WLAN-Hotspots ihr Notebook direkt dem Internet aussetzen, machen sie auf jeden Fall Sinn. Auch hier gilt, dass eine zentral gemanagte Version, bei der der Benutzer keine Einflussmöglichkeiten hat, einer rein lokalen Installation vorzuziehen ist.

Optional können Sie auch die Funktionen von Windows nutzen. Da ist einerseits die Internet-Verbindungs-Firewall, die eingehende Verbindungsabfragen für nicht konfigurierte Dienste ablehnt, und der TCP/IP-Paketfilter, bei dem Sie global festlegen, welche TCP/IP-Ports überhaupt auf dem Rechner erreicht werden können.

Auf der Wählverbindung sollten ohnehin generell der "Windows-Client" und die "Datei- und Druckerfreigabe für Microsoft Netzwerke" deaktiviert sein.

6. Weitere Punkte

Stellen Sie Verhaltensmaßregeln und Anleitungen für das mobile **Surfen im Internet**¹⁰ bereit. Lassen Sie sich diese Regeln von der Geschäftsführung und dem Betriebsrat absegnen und sprechen Sie auch einen Maßnahmenkatalog für Verstöße ab. Die Erfahrung zeigt, dass ein Appellieren an die Vernunft des Benutzers nicht immer ausreichend ist, um die Sicherheit zu gewährleisten - direkte Konsequenzen aus Fehlverhalten dagegen schon. Regelmäßige Schulungen gehören übrigens auch dazu.

Lassen Sie die Möglichkeit nicht außer Acht, dass ein mobiles Gerät gestohlen wird oder verloren geht. Ausreichende Absicherung durch **starke Passwörter**¹¹, **Verschlüsselung sensibler Daten auf dem Notebook**¹² und die **gründliche Löschung von Dateien**¹³ sind hier das Mindestmaß. Das gilt ganz besonders, wenn das Gerät für den Einsatz in einem VPN vorgesehen ist, ansonsten stehen einem Dieb alle Möglichkeiten in Ihrem Netzwerk offen.

Manager haben gerne die Kontrolle, auch über Dinge, von denen sie nicht genug Ahnung haben. So wird es Ihnen als Administrator oder Sicherheitsverantwortlicher mit großer Wahrscheinlichkeit passieren, dass sich Ihr Geschäftsführer nicht in der Benutzung des Notebooks einschränken lassen will oder ihm all die Maßnahmen zu mühsam sind. Sprich: Die Manager wollen die volle Kontrolle über "ihr" Notebook und so wenig Beeinträchtigung durch Sicherheitsmaßnahmen wie möglich. Lassen Sie sich nicht einschüchtern, denn wenn etwas schief geht, rollt Ihr Kopf - und im schlimmsten Fall sind Sie auch noch schadenersatzpflichtig.

7. Sicherheitsvorkehrungen im LAN

Auch im Netz sollten Sie nicht auf entsprechende Sicherungsmaßnahmen verzichten, da sich neue Viren oder Exploits trotz aller Vorkehrungen auf dem mobilen Arbeitsplatz eingemischt haben können. Der erste Schritt sollte daher sein, das Paradigma "Wer im LAN ist, dem vertrauen wir" zu den Akten zu legen. Wenn Ihre Infrastruktur beispielsweise VLANs unterstützt, können Sie alle Notebooks in einem separaten Netz sammeln, das durch ein Security-Gateway vom normalen LAN abgekoppelt ist.

Sind VLANs nicht möglich, können Sie das Netz immer noch über die Verkabelung und die Platzierung der Switches so strukturieren, dass zwei verschiedene physikalische LANs existieren, die durch ein Security-Gateway verbunden sind.

VPN-Verbindungen sollten Sie übrigens ebenfalls nicht direkt im LAN enden lassen, sondern auch als "untrusted" betrachten und über ein Gateway abkoppeln. Das entfernte Gerät könnte ja jederzeit infiziert sein und ein Trojaner oder Virus über das Gerät Zugang erlangen. Dasselbe gilt für WLAN-Access-Points im LAN. Auch wenn Sie alles Mögliche getan haben, um die Funkstrecke abzusichern: Lieber etwas paranoid, als komplett kompromittiert.

Mit NAC (Network Admission Control, Network Access Control) oder NAP (**Network Access Protection**¹⁴) stehen weitere Verfahren zur Verfügung, mit denen sich verhindern lässt, dass ungenügend geschützte Systeme ins LAN gelangen. Dabei werden Clients während der Authentifizierung auch zusätzlich auf ihren „Gesundheitszustand“ geprüft. Überprüft wird beispielsweise, ob alle Patches eingespielt sind, der Virens Scanner auf dem neuesten Stand ist oder bestimmte Systemeinstellungen den Richtlinien entsprechen.

Stellt das System eine Verletzung der vom Administrator festgelegten Regeln fest, wird der Client zunächst unter Quarantäne gestellt und an einen so genannten Remediation-Server verwiesen. Von dort erhält der Client die relevanten Updates und Signaturen. Erst wenn er dann als „sauber“ eingestuft ist, darf der Client ins normale Netzwerk. Kann das nicht sichergestellt werden, bleibt der Client mit eingeschränkten Rechten in isolierter Quarantäne oder wird ganz blockiert. Isolation heißt, dass die Clients auch nicht untereinander kommunizieren können. Andernfalls könnten sie sich gegenseitig infizieren!

8. Fazit

War früher noch die zu schützende Netzwerk-Grenze der mit dem Internet verbundene Router, so gestaltet sich die Situation inzwischen sehr vielschichtig. Im Prinzip ist jede einzelne Station so abzusichern, als gäbe es keine weitere Verteidigung gegen Malware, Hacker oder menschliches Versagen.

Eine Vielzahl von gesetzlichen und sonstigen Regelwerken nimmt den Administrator in die Pflicht, aber auch die Geschäftsführung. Aber allein der gesunde Menschenverstand sollte jedem deutlich machen, dass Sicherheit eine essenzielle Grundvoraussetzung für den Betrieb einer jeglichen IT ist: Produktionsausfälle kosten Geld, verlorenes Vertrauen der Kunden (etwa aufgrund einer Datenschutzpanne) kostet Aufträge (und damit Geld) und Entwicklungen oder sonstige kritische Informationen in den falschen Händen können im schlimmsten Fall sogar die Existenz bedrohen. (mha)

Links im Artikel:

¹ <https://www.tecchannel.de/news/20030812/thema20030812-11512.html>

² <https://www.tecchannel.de/link.cfm?pk=430834>

³ <http://windowsupdate.microsoft.com/>

⁴ <https://www.tecchannel.de/link.cfm?pk=481640>

⁵ <http://www.safer-networking.org/de/index.html>

⁶ <https://www.tecchannel.de/link.cfm?pk=401894>

⁷ <https://www.tecchannel.de/link.cfm?pk=445486>

⁸ <https://www.tecchannel.de/link.cfm?pk=445486>

⁹ <https://www.tecchannel.de/link.cfm?pk=402411>

¹⁰ <https://www.tecchannel.de/link.cfm?pk=401881>

¹¹ <https://www.tecchannel.de/link.cfm?pk=402350>

¹² <https://www.tecchannel.de/link.cfm?pk=481635>

¹³ <https://www.tecchannel.de/link.cfm?pk=402093>

¹⁴ <https://www.tecchannel.de/link.cfm?pk=462287>

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.