Fast Facts:

- Internet-Sperren sind ein beliebtes Mittel, um im Unternehmen Mitarbeiter von privaten Webseiten fernzuhalten.
- Die Top 3 der gesperrten Dienste sind Filesharing, soziale Netzwerke und Online-Games.
- Der Artikel erklärt, dass Sperren allein kein Allheilmittel sind und wie man trotzdem Sicherheit im Unternehmen gewährleistet.
- Zeichen: 5.167 mit Leerzeichen

Ohne Internet geht im Büro nichts mehr. Aber die Vielfalt an Diensten kann den Arbeitsfluss auch merklich bremsen. Internet-Sperren scheinen da das Mittel der Wahl zu sein. Allein bringen sie aber nicht immer den gewünschten Effekt. Der Artikel erklärt, wie man sich vor Internet-Bedrohungen schützt.

Schutz vor den bösen Drei

Filesharing, Social Networks, Online-Games, das sind die Top-Drei der gesperrten Internet-Dienste in Unternehmen. Doch ist ein Verbot wirklich der beste Schutz?

Die Spielregeln für die Internet-Nutzung im Büro legen die Unternehmen fest. Dabei ist es in vielen Firmen an der Tagesordnung, für den Betrieb nicht nötige Webdienste einfach zu sperren. Die Argumente dafür sind vielfältig, meist wird mit Millionenverlusten argumentiert, die abgelenkte Mitarbeiter verursachen [1]. Nach den Ergebnissen einer weltweiten Umfrage von Kaspersky sind die am häufigsten gesperrten Dienste Filesharing, soziale Netzwerke und Online Games. Doch sind Sperren allein immer die richtige Maßnahme? Nein, ganz sicher nicht.

Sperren sind nur eine Möglichkeit, um Mitarbeiter davon abzuhalten, während der Arbeitszeit private Dinge im Internet zu erledigen. Sie bieten einige Vorteile: Beispielsweise zeigen sie den Mitarbeitern sehr direkt, dass die gesperrten Dienste während der Arbeitszeit nicht erwünscht sind. Außerdem sind speziell die genannten

drei Dienste eine gern genutzte Spielwiese von Malware-Autoren, die über diese Wege Computer zu infizieren versuchen. Und wo kein Dienst genutzt werden kann, da kann auch kein Schädling Schaden anrichten. Es gibt aber auch Nachteile von Sperren: So könnten sich einige Mitarbeiter herausgefordert fühlen, die Administratoren zu überlisten und trotzdem die Dienste ihrer Wahl zu nutzen. Dann wiegt man sich als Sicherheitsverantwortlicher sogar in falscher Sicherheit, denn schließlich geht man davon aus, dass man etwa keine Probleme mit Malware auf sozialen Netzwerken hat. Der größte Nachteil entsteht aber, wenn Internet-Sperren einfach so aufgebaut werden, ohne den Nutzer ins Boot zu holen. Die gleiche Situation entsteht, wenn in der Kantine plötzlich nicht mehr drei Gerichte zur Auswahl stehen, sondern nur noch Einheitsbrei. Die Nutzer sind erst frustriert und nehmen dann die Vorgaben des Unternehmens nicht mehr ernst.

Doch Moment: Klar ist, kein Unternehmen kann es dulden, dass seine Mitarbeiter den ganzen Tag in Filesharing-Netzen unterwegs sind, in Facebook chatten und sich alle zehn Minuten in Online-Games duellieren. Doch es gibt Alternativen oder zumindest Ergänzungen zu Internet-Sperren. Die Dienste gehören klar in den Bereich der Sicherheitsstrategie. Dort sollten aber neben technischen Schutzsystemen und Notfallplänen auch Mitarbeiter auftauchen, ein wichtiger Punkt der in der Regel fehlt. Doch ohne sicherheitsbewusstes Personal ist jede Security-Strategie zum Scheitern verurteilt. Dabei ist es ganz einfach, seine Mitarbeiter mit ein paar Tricks in die Security-Strategie einzubinden.

Schulungen anbieten

Wenn es eine neue Office-Version gibt, steht eine Schulung für die Mitarbeiter wie selbstverständlich auf dem Plan. Warum also nicht auch bei neuen Sicherheitsbedrohungen? Doch Vorsicht, dazu gehört nicht jede neue Malware im Detail. Als Verantwortlicher für Sicherheitsschulungen müssen Sie das Thema mit vielen Praxis-Beispielen und Tipps unterfüttern, etwa wie man seine Passwörter sicher im Griff hält oder welche Risiken soziale Netzwerke haben.

Kommunikation schützen

Sicherheits-Software schützt heute sehr zuverlässig vor Malware. Aber das ist kein Freifahrtschein, alle Sicherheitsbedenken fallen zu lassen. Klären Sie Ihre Mitarbeiter

über sichere Kommunikation auf und geben Sie ihnen ein paar Tipps mit. Dazu gehört etwa der sichere Umgang mit Mails. Klären Sie Ihre Mitarbeiter auf, wie viele Spam-Mails die Filter jeden Tag abhalten. Wer etwa das Verschicken von EXE- und ZIP-Dateien blockiert, kann hier mit plakativen Beispielen den Hintergrund erklären. Zeigen Sie Alternativen auf, etwa den Dateitausch via Secure FTP oder über Projektmanagement-Software. Der Grund: Mitarbeiter sollten den Malware-Schutz der Firmen-Mails nicht durch die Nutzung privater Webmailer unterlaufen. Wichtig: Nutzen Sie Schulungen auch, um etwa zu zeigen, wie das Verschlüsseln und Signieren von Mails funktioniert.

Sicher im Messenger

Zeigen Sie Ihren Mitarbeitern, dass es auch Messenger-Spam gibt und dass viele Phishing-Attacken auch über Messenger-Netzwerke laufen. Würmer, etwa aus der Zeroll-Familie, verbreiten sich sofort über die komplette Kontaktliste eines Nutzers. Neu ist, dass nicht nur ein Messenger-Netzwerk betroffen ist, sondern Zeroll mehrere Protokolle spricht. Köder sind hier Links zu "interessanten" Bildern, die in Wahrheit zu einer infizierten Datei führen. Diese Datei ist nicht nur für die Verbreitung zuständig, sondern öffnet auf dem befallenen PC auch eine Hintertür.

Soziale Netzwerke sicher nutzen

Auch wenn Facebook & Co. in der Firma nicht erlaubt sind, Business-Netzwerke wie Xing sind geschäftsrelevant und aus vielen Unternehmen nicht mehr wegzudenken. Los geht es schon mit dem richtigen Umgang mit den Zugangspasswörtern. Diese sollten nicht im Browser gespeichert werden. Klären Sie Ihre Mitarbeiter über die Preisgabe von Informationen auf und zeigen Sie verschiedene Freigabestufen. Natürlich kann man seine Mail-Adresse und Telefonnummer für Geschäftskontakte freigeben, eine normale Google-Suche sollte diese Daten aber nicht ausspucken.

[1] http://harmon.ie/Company/PressReleases/press-release-may-18-2011

Other useful links:
www.securelist.com/en/analysis
www.kaspersky.com