# Sicherheit

Ein Anwender meldet sich an seinem System mit "administrator" ohne Passwort an. Sein WLAN verschlüsselt er mit WEP, sein Betriebssystem ist Windows XP, Service Pack 1, sein Browser ist der Internet Explorer 5.5. Welche Sicherheitsprobleme sehen Sie? Wie kann er seine Systemsicherheit erhöhen? Geben Sie mind. 5 Verbesserungsvorschläge an und erläutern Sie diese jeweils kurz.

Sicherheitsprobleme

* Kein Passwort: ein Angreifer kann sich einfach einloggen
* WEP: gilt als gebrochen (RC4 mit schwachem Schlüsselmanagement mit 40 Bit Schlüssellänge, verwendet statischen Schlüssel, Initialisierungsvektor im Klartext)
* Altes Betriebssystem: wird nicht mehr sicherheitsmäßig gewartet, außerdem wurde es nie aktualisiert (Service Pack 1), sodass Sicherheitsverbesserungen neuerer Versionen nicht installiert wurden
* Internet Explorer: alt, keine ausreichende Sicherheit

Verbesserungsvorschläge

* Separaten Benutzer mit eingeschränkten Berechtigungen verwenden, sodass bei kritischen Aktionen immer erst das Administrator-Passwort eingegeben werden muss
* Dem Administrator-Benutzer und dem „normalen“ Benutzer sollte zudem ein sicheres Passwort zugewiesen werden (Kombination aus Groß-/Kleinschreibung, Zahlen und Sonderzeichen, mindestens 8 Zeichen)
* Bei dem WLAN sollte stattdessen WPA2 (AES Verschlüsselung 256 Bit) verwendet werden in Zusammenhang mit einem sicheren Passwort
* Es sollte ein aktuelles Betriebssystem verwendet werden z.B. Windows 10, sowie regelmäßig aktualisiert werden
* Der installierte Browser sollte aktualisiert werden auf die neuste Version
* Außerdem macht es Sinn, einige Sicherheitseinstellungen des Browsers zu aktivieren
* Die Fernkonfiguration des Routers sollte deaktiviert werden, sodass nur eine Konfiguration innerhalb des lokalen Netzes möglich ist
* Es sollte eine Firewall eingesetzt werden, wobei nur die wirklich vorgesehene Kommunikation erlaubt wird und alles andere verboten wird, sodass sich dem Angreifer wenig Angriffsfläche bietet
* Es ist sinnvoll ein Intrusion Detection System (IDS) oder Intrusion Prevention System (IPS) einzusetzen, damit Angriffe erkannt und abgewehrt werden