Risikoanalyse

Patrick Bucher

12.03.2017

Risiken

a. Ein Nachbar (oder dessen verwurmter PC) könnte die WEP-WLAN-Verschlüsselung knacken. Dadurch ergeben sich die folgenden Risiken:
    1. Der Drucker könnte von Unbefugten verwendet werden. Das bringt diesen zwar nichts, könnte aber Papier und Toner bzw. Tinte verschwenden und das Gerät abnutzen.
    2. Die beiden installierten Kameras könnten zur Spionage verwendet werden. Das bedeutete einerseits die Verletzung der Privatsphäre, andererseits könnte dies auch für Einbrüche nützlich sein, da man so herausfinden kann, wann niemand zu Hause ist.
    3. Besteht erst einmal Zugriff auf den Router und erlaubt dieser Konfiguration über WLAN, könnte ein Angreifer auf sämtliche ungeschützten Freigaben im Netzwerk zugreifen.
    4. Weiter könnten Geräte per MAC-Sperre aus dem Netzwerk ausgeschlossen werden.
    5. Das Netzwerk könnte so gänzlich lahmgelegt werden.
    6. Der Router könnte durch Einspielung einer manipulierten Firmware gar zerstört werden.
    7. Über das gekaperte Netzwerk könnten trojanische Pferde eingespeist werden, die dann Remote-Kontrolle über die Systeme übernehmen könnten. Dadurch könnten private Daten abgegriffen und/oder gelöscht werden.
    8. Die Windows-Intallationen könnten unwiderruflich zerstört werden.

b. Onkel Özutöcks Laptop könnte verwurmt sein.
    9. Die Programme, die er so auf die PCs überspielt, könnten dadurch ebenfalls verwurmt sein.

c. Es ist nirgends die Rede von Antiviren-Software. Doch Windows ist aufgrund seiner Verbreitung ein beliebtes Ziel für Entwickler von Schadsoftware. Von Datensicherung ist auch nirgends die Rede.
    10. Mit sogenannter Ransomware könnten private Daten verschlüsselt werden, sodass sie nur durch eine Lösegeldzahlung entschlüsselt werden könnten. Es droht Datenverlust oder finanzieller Schaden.
    11. Trojanische Pferde oder Würmer könnten aktive Logins (über Session-Cookies) übernehmen und auf verschiedenen Benutzerkonti straftrechtlich relevante Informationen verbreiten (Facebook, Twitter) oder im schlimmsten Fall sogar auf das Online-Banking zugreifen. Sind die Passwörter im Klartext abgespeichert, können sie alle problemlos abgegriffen werden.

12. Bei einem plötzlichen Festplatten-Crash gehen die darauf gespeicherten Daten unwiderruflich verloren. Daten könnten auch aus Versehen gelöscht werden. Wird dies lange nicht bemerkt, kann die Wiederherstellung der Daten scheitern.

d. Arbeitet Herr Meier zu Hause, dürften vertrauliche Daten der Bundesverwaltung betroffen sein.
    13. Es könnten vertrauliche Daten oder gar Staatsgeheimnisse an Unbefugte gelangen. Herr Meier könnte im schlimmsten Fall der Veruntreuung oder gar des fahrlässigen Landesverrats angeklagt werden. (Die Verwendung von WEP zur Sicherung eines WLAN ist fahrlässig.)

e. Die jüngste Tochter Dora (12) kann vielleicht die Risiken nicht abschätzen, die ein Smartphone mit Kamera mit sich bringen.
    14. Pädophile könnten sie nach Bildern und nach ihrer Adresse fragen, wodurch sie direkt gefährdet werden könnte.
    15. Bilder, die nicht für die Öffentlichkeit bestimmt sind, könnten auf soziale Medien gelangen, wo sie kaum mehr gelöscht werden könnten.

Risikogewichtung

Risiko	Häufigkeit	Schadensausmass	Risiko
1. Unbefugter Druckerzugriff	1	1	1
2. Unbefugter Kamerazugriff	1	3	3
3. Unbefugter Routerzugriff	2	1	1
4. MAC-Aussperrung	1	1	1
5. Netzwerk-Lahmlegung	1	1	1
6. Router-Zerstörung	1	1	1
7. Unbefugter Datenzugriff	1	3	3
8. Windows-Zerstörung	2	2	4
9. PC-“Verwurmung”	3	2	6
10. Ransomware	2	3	6
11. Identitätsdiebstahl	2	3	6
12. Datenverlust	3	2	6
13. Datendiebstahl	1	3	3
14. Pädophile Übergriffe	1	3	3
15. Ungewollte Foto-Veröffentlichung	3	2	6