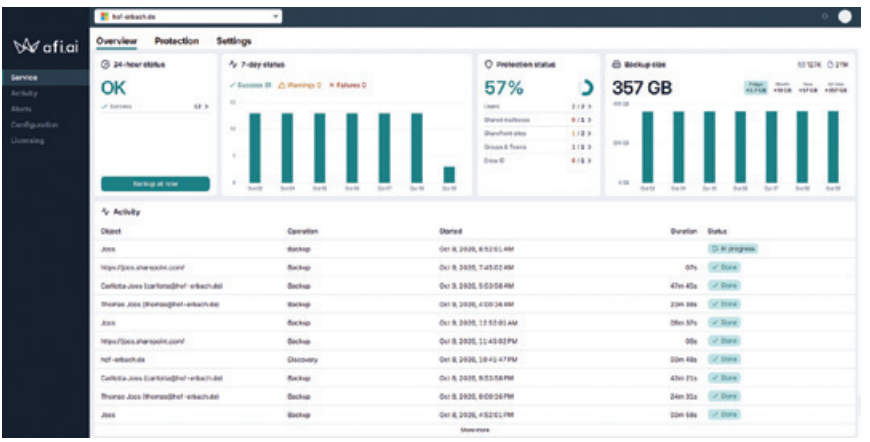
So sichert man Router, Büro-PC und Diensthandy ab

Ein Router mit Werkspasswort, ein Büro-PC mit Windows 10 und ein Diensthandy mit hinterlegtem Mailpasswort verschaffen Angreifern Zugang zum Betrieb. Der Beitrag zeigt, welche Einstellungen der Inhaber selbst vornehmen kann und was er besser dem IT-Dienstleister überläßt … | VON THOMAS JOOS

Gut jeder dritte von 200 Handwerksbetrieben, die Techconsult im Auftrag von Sophos zum Jahreswechsel 2025/26 befragt hat, rechnet nach einem Cyberangriff mit eingeschränktem Betrieb oder längeren Ausfällen (*https://www.sophos.com/de-de/blog/how-well-prepared-are-craft-businesses-for-cyber-incidents*). Knapp drei von zehn Betrieben schützen nur Teile ihrer Geräte und Programme.

Die FRITZ!Box installiert neue Software selbst

Das BSI rät, bei jedem Router automatische Updates einzuschalten. Bei der FRITZ!Box prüft der Inhaber unter „System“ -> „Update“ -> „Auto-Update“, ob die Werkseinstellung Stufe III aktiv ist. Neue Versionen ihrer Software FRITZ!OS installiert die Box nach einigen Wochen selbst (*https://fritz.com/pages/online-update*). Für die älteren FRITZ!Box-Geräte, wie zum Beispiel 7560 nennt der Hersteller FRITZ!OS 7.30 als neueste Version, für die 7590 dagegen FRITZ!OS 8.25. Erhält ein Router keine neuen Versionen mehr, ist ein Austausch ratsam. Beim Neukauf hilft das IT-Sicherheitskennzeichen des BSI.



Der Router bekommt ein neues Passwort

Das Werkspasswort des Routers sollte der Inhaber nach der ersten Anmeldung ändern. Für das WLAN, also das Funknetz im Büro, empfiehlt sich die Verschlüsselung WPA3, bei älteren Geräten WPA2, sowie ein Passwort mit mindestens 20 Zeichen.

Kunden erhalten ein Gastnetz ohne Zugang zum Firmennetz. Für den Zugriff von unterwegs richtet der IT-Dienstleister ein VPN ein, eine verschlüsselte Verbindung ins Büronetz.

Die Telefonanlage sperrt teure Rufnummern

Nach einem unbefugten Zugriff auf den Router können Angreifer über die Telefonanlage am

Router unbemerkt teure Auslands- und Sonderrufnummern wählen, die Rechnung geht an den Betrieb. Die Bundesnetzagentur rät, ungenutzte Zielrufnummern in Router oder Telefonanlage zu sperren. Nummern wie (0)900 sperrt der Telefonanbieter auf Wunsch kostenlos im Netz (*https://www.bundesnetzagentur.de/routerhacking*).

Der Büro-PC erhält Updates und eigene Konten

Seit dem Supportende im Oktober 2025 erhalten Betriebe Sicherheitsupdates für Windows 10 nur über das Programm Extended Security Updates (ESU), für das Microsoft im ersten Jahr 61 US-Dollar je Gerät verlangt und dessen Preis sich jährlich verdoppelt. Nach höchstens drei Jahren endet die Versorgung, ein späterer Einstieg kostet die verpaßten Jahre mit (*https://learn.microsoft.com/de-de/windows/whats-new/extended-security-updates*). Für drei Büro-PCs summiert sich das bis Oktober 2028. Den Umstieg auf Windows 11 plant der IT-Dienstleister.

Jeder Mitarbeiter sollte ein eigenes Konto ohne Administratorrechte nutzen, also ohne das Recht, Programme zu installieren. Ein versehentlich gestartetes Schadprogramm erhält so nur diese Rechte. Für das Mailpostfach lohnt sich die Zwei-Faktor-Anmeldung, bei der das Postfach neben dem Passwort einen Code vom Smartphone abfragt. Ein erbeutetes Passwort allein reicht dann nicht mehr für die Anmeldung.

Diensthandys aktualisieren sich automatisch

Am iPhone schaltet der Inhaber unter „Einstellungen“ -> „Allgemein“ -> „Softwareupdate“ -> „Automatische Updates“ die Option „Automatische Installation“ ein. Das iPhone installiert neue Versionen nachts beim Laden im WLAN.

Unter Android zeigt „Einstellungen“ -> „System“ -> „Softwareupdates“ den Stand, wobei Aktualisierungen vom Mobilfunkanbieter und vom Hersteller abhängen (*https://support.google.com/android/answer/7680439?hl=de*). Beim Kauf eines Diensthandys lohnt deshalb die Frage, wie lange der Hersteller das Gerät aktualisiert. Eine Bildschirmsperre mit PIN schützt das Firmenpostfach, falls ein Diensthandy verloren geht. Das Sperren und Löschen über eine zentrale Geräteverwaltung beschreibt der Baustellen-Beitrag in CiH-Ausgabe 8-9/26 (*www.handwerke.de/pdf/CIH_8-9-26_Digi-Hard_Baustelle-absichern.pdf*).

Die Sicherung lagert an einem zweiten Ort

Nach einem Wasserrohrbruch, Ransomware-Befall oder Löscheinsatz der Feuerwehr bleibt nur eine Datensicherung außerhalb des Betriebs erhalten.

WAS WER AN WELCHEM GERÄT EINSTELLT

Gerät	Einstellung	Wer
Router	Neues Passwort, WPA3, Gastnetz, VPN	Inhaber, VPN der IT-Dienstleister
Router-Software	Auto-Update einschalten, alte Modelle austauschen	Inhaber
Telefonanlage	Ungenutzte Zielrufnummern sperren	Inhaber
Büro-PC	Windows 11 oder ESU, Konto ohne Administratorrechte	IT-Dienstleister
Mailpostfach	Zwei-Faktor-Anmeldung	Inhaber
Diensthandy	Automatische Updates, Bildschirmsperre mit PIN	Inhaber
Datensicherung	Medium trennen, Kopie außerhalb, Probe	Inhaber

Quelle: BSI, FRITZ!, Microsoft, Bundesnetzagentur, Zusammenstellung Thomas Joos

Das Speichermedium sollte der Inhaber nach jeder Sicherung vom Rechner trennen, damit Ransomware, also Erpressersoftware, die Kopie nicht mit verschlüsselt. Bei einer regelmäßigen Probe holt er eine Datei aus der Sicherung zurück. Das regelmäßige Testen der erfolgreichen Wiederherstellung ist bei Backups ein wichtiger Faktor.

Den Gesamtstand mißt der CyberRisikoCheck nach DIN SPEC 27076. Ein IT-Dienstleister prüft darin in einem Interview von ein bis zwei Stunden 27 Anforderungen und übergibt einen Bericht mit Empfehlungen, sortiert nach Dringlichkeit (*https://www.bsi.bund.de/dok/crc*).