

Beispiel Berlin-Hack: Der Angriff, den Sie selbst starten



Was ist passiert?

Im August 2026 wurden die Senatsverwaltungen für Stadtentwicklung, Bauen und Wohnen sowie für Mobilität, Verkehr, Klimaschutz und Umwelt vom Berliner Landesnetz getrennt. Nach Berichten des BSI begann der Angriff mit TerminalFix, einer Weiterentwicklung von ClickFix. Die Täter, nach eigenen Angaben die Gruppe Rhysida, erbeuteten Daten im Terabyte-Bereich und erpressten das Land.

Dazu brauchten sie keine Sicherheitslücke: Ein Mensch führte den Befehl selbst aus.

Was Sie sehen	Was im Hintergrund passiert
1 Link, Phishing-Mail oder präparierte Webseite	Sie landen auf einer Täuschungsseite
2 „Bestätigen Sie, dass Sie ein Mensch sind“	Ein Schadbefehl wird in die Zwischenablage kopiert
3 Anweisung: Tastenkombination drücken, dann Strg+V drücken, Enter	Sie starten die Schadsoftware, Virenschutz greift oft zu spät
4 Nichts Auffälliges	Dauerhafter Fernzugriff auf das System

Warnsignale

- Eine Webseite oder Mail fordert Sie auf, unbekannte Tastenkombinationen zu drücken (z. B. **⌘**+R, **⌘**+Leertaste, F12, **⌘**+X, ...).
- Sie sollen Text kopieren, einfügen oder eintippen – in ein Terminal, ein Eingabefenster, die Browser-Konsole oder Entwicklertools.
- Sie sollen ein Programm oder Fenster öffnen, das Sie sonst nie benutzen, um ein „Problem zu beheben“.
- Der Auslöser wirkt harmlos: Captcha, „Fehlermeldung“, „Update nötig“, „Dokument kann nicht angezeigt werden“, Gewinn- oder Support-Versprechen.

Das sollten Sie tun

1. **Abbrechen:** Nichts drücken, nichts einfügen, Tab/Browser schließen.
2. **Nichts ausgeführt?** Zwischenablage leeren (z. B. etwas Harmloses kopieren) und melden.
3. **Doch ausgeführt?** **Sofort** Netzkabel ziehen bzw. WLAN trennen, Gerät **nicht** ausschalten, **sofort melden**.
4. **Passwörter** von einem **sauberen Gerät** aus ändern.

Fragen?

Sie erreichen uns jederzeit per E-Mail unter informationssicherheit@tu-freiberg.de, weitere Informationen und Aktuelles finden Sie auf <https://tu-freiberg.de/informationssicherheit>.

Rechts: Beispiele für präparierte Webseiten für Terminalfix und Clickfix. Angreifer können Betriebssystem und Sprache automatisch erkennen und so besonders treffsicher überzeugende Fälschungen erstellen.

