

03.06.2008

<http://frontal21.zdf.de/ZDFde/inhalt/18/0,1872,7246834,00.html>



ZDF

Datenfalle Kopierer

Sicherheitsrisiko Kopierer

Sicherheitslücke wird unterschätzt

von *Susanne Härpfer und Andreas Halbach*

Fotokopierer gehören längst zum modernen Büroalltag. Sie sind inzwischen in beinahe jedem Unternehmen und jeder Behörde zu finden. Was jedoch kaum jemand weiß: Fotokopierer stellen für IT-Experten eine der größten Sicherheitslücken im Datenschutz dar. Sie warnen: "Die Geräte laden zum Angriff ein."

"Früher waren Drucker nur Drucker und keine Computer", sagt Patrick Hof, IT-Sicherheitsexperte bei der Firma "RedTeam Pentesting" in Aachen. "Viele Fotokopierer stehen auf dem Gang. Ich komme direkt an die Geräte ran, sie stehen an exponierter Stelle, als Angreifer kann ich viel machen."

ZITAT

„Wir wären natürlich in der Lage, alle Kopien, die hier gemacht werden, von den letzten zwei oder drei Wochen zu reproduzieren.“

Keine Datensicherheit im Copy-Shop

Und so ist es für professionelle Computer-Hacker leicht, sämtliche kopierte Daten abzugreifen. Auch Kunden von Copy-Shops sind vor Missbrauch ihrer Daten nicht geschützt. Denn die heutzutage gebräuchlichen digitalen Multifunktionsgeräte sind mit Festplatten ausgestattet, auf denen pro Gerät mehr als 10.000 Kopien gespeichert werden können. Diese Kopien lassen sich von Profis leicht wieder herstellen und ausdrucken. Das bestätigt auch ein Mitarbeiter eines Copy-Shops, der nicht genannt werden möchte, auf Nachfrage von Frontal21.

"Wir wären natürlich in der Lage, alle Kopien, die hier gemacht werden, von den letzten zwei oder drei Wochen zu reproduzieren. Aber nach der Datensicherheit hier im Copy-Shop fragt doch niemand. Auch unsere Kunden interessiert das nicht."

"Das ist bedenklich"

Tatsächlich aber sind die Kunden entsetzt, ahnten sie doch bisher nicht, dass ihre Daten in den meisten Copy-Shops nicht sicher sind. "Das ist aber

bedenklich", so ein Kunde. "Ich bin Lehrer und kopiere hier auch Daten und Fotos meiner Schüler. Das finde ich aber nicht gut, wenn das hier nicht sicher ist."

Wie einfach es ist, selbst an sensible Daten von Unternehmen, Behörden und Forschungseinrichtungen heranzukommen, zeigt unser Praxistest, bei dem uns Spezialisten von "RedTeam Pentesting" unterstützen. Die Firma aus Aachen berät große Konzerne und Banken in Sachen Netzwerksicherheit.

Zugangscode aus dem Internet

Der Datenschutzbeauftragte des Landes Schleswig-Holstein erlaubt uns, seinen Kopierer anzugreifen. Dazu besorgen sich unsere Hacker zunächst den Zugangscode für das Gerät - ganz einfach aus dem Internet. Hier sind zum Beispiel Benutzerhandbücher zu den gängigen Typen zu finden.

ZITAT

„Wir kennen zwar im Prinzip die Angriffsmöglichkeiten, aber dass es so leicht ist, an die Geräte heranzukommen, das war nicht bekannt.“

Thilo Weichert

"Ich gebe den Admin-Code ein, der für den Servicetechniker gedacht ist. Jetzt habe ich die Kontrolle erlangt und bin selbst Administrator. Das ganze hat nur ein paar Sekunden gedauert", erklärt Patrick Hof. Von nun an hat unser Hacker die Kontrolle über sämtliche Daten, die über dieses Gerät laufen. Alle Kopien, Scans und Ausdrücke kann er von seinem Notebook aus umlenken, manipulieren, verändern oder ausdrucken. Da schützt auch kein eigens für die Sicherheit eingerichteter PIN-Code. Selbst den können unsere Profis mühelos knacken.

Angriffe auch von außen möglich

Damit hat der Landesbeauftragte für Datenschutz, Dr. Thilo Weichert, nicht gerechnet. "Wir kennen zwar im Prinzip die Angriffsmöglichkeiten, aber dass es so leicht ist, an die Geräte heranzukommen, die Rechte zu übernehmen, das war nicht bekannt. Ich bin schockiert über das Ergebnis."

Doch damit nicht genug. Ein Angriff dieser Art ist selbst möglich, ohne dass die Hacker das Gebäude ihres Opfers überhaupt betreten. "Es gehört zu unserer täglichen Arbeit, dass wir auch komplett von außerhalb zugreifen. Das klappt in vier von fünf Fällen", erklärt Hof.

Hersteller spielen Gefahr herunter

Doch die Hersteller spielen die Gefahr herunter, verweisen darauf, dass sie auch verschlüsselte Festplatten anbieten. Doch nach Recherchen von Frontal21 sind nur die allerwenigsten der verkauften Kopierer auf diese Weise geschützt. Zudem ist dies kein Allheilmittel. Frontal21 zeigt: Hacker können die Daten sogar abgreifen, bevor sie überhaupt auf der Festplatte ankommen.

So ist viel Aufklärung und technische Aufrüstung notwendig, um die bislang weithin unterschätzte Sicherheitslücke bei den Kopierern zu schließen.