Ransomware victims thought their backups were safe. They were wrong

By Steve Ranger

Published: 2020-02-27 · Archived: 2026-04-06 00:58:22 UTC

The UK's cybersecurity agency has updated its guidance on what to do after a ransomware attack, following a series of incidents where organisations were hit with ransomware, but also had their backups encrypted because they had left them connected to their networks.

Keeping a backup copy of vital data is a good way of reducing the damage of a ransomware attack: it allows companies to get systems up and running again without having to pay off the crooks. But that backup data isn't much good if it's also infected with ransomware -- and thus encrypted and unusable -- because it was still connected to the network when the attack took place.

The UK's National Cyber Security Centre (NCSC) said it has now updated its guidance by emphasising offline backups as a defence against ransomware.

"We've seen a number of ransomware incidents lately where the victims had backed up their essential data (which is great), but all the backups were online at the time of the incident (not so great). It meant the backups were also encrypted and ransomed together with the rest of the victim's data," the agency warned.

SEE: A winning strategy for cybersecurity (ZDNet special report) | Download the report as a PDF (TechRepublic)

While the NCSC has previously recommended offline backups, it said recent incidents, such as attacks by the Trickbot banking trojan malware, suggested greater emphasis was needed.

The key to mitigating a ransomware attack, NCSC said, is to ensure that businesses have up-to-date backups of important files. Organisations should ensure that a backup is kept separate from their network -- offline -- or in a cloud service designed for this purpose.

However, NCSC warned that cloud-syncing services (like Dropbox, OneDrive and SharePoint, or Google Drive) should not be used as the only backup, in case they automatically synchronise immediately after files have been 'ransomwared', at which point the synchronised copies are lost as well.

The agency also recommends that the device containing any backup, like an external hard drive or a USB stick is not permanently connected to your network and that multiple copies exist.

NCSC also warned: "An attacker may choose to launch a ransomware attack when they know that the storage containing the backups is connected."

SEE: Six suspected drug dealers went free after police lost evidence in ransomware attack

In a separate advisory on offline backups, NCSC notes that it has seen numerous incidents where ransomware has not only encrypted the original data on-disk, "but also the connected USB and network storage drives holding data backups. Incidents involving ransomware have also compromised connected cloud storage locations containing backups."

The most common method for creating resilient data backups, NCSC said, is to follow the '3-2-1' rule: at least three copies, on two devices, and one offsite.

Editorial standards
