+44 345 094 0945
www.waterstons.com
Article

Cyber Report Spotlight: Microsoft internal files accidentally exposed to the internet

Breadcrumb

Insight navigation

Download PDF

May 2024

Cyber Report Spotlight: Microsoft internal files accidentally exposed to the internet

In this month's cyber report we delved into a recent cyber security risk at Microsoft where an improperly configured server left internal Microsoft data, including passwords, exposed online.

Categories Cyber Resilience

May 2024

What happened

On February 6th, security researchers discovered that an internal Microsoft storage server, hosted within Azure, was publicly accessible online. The server did not require any authentication, exposing the sensitive data to anyone who found it.

The server contained data related to Microsoft's Bing search engine, including code, scripts, and configuration files, some of which contained credentials and keys for internal systems.

Although the exposed server was reported on February 6th, it was only secured on March 5th - almost a month later. It is unknown how long the server was exposed for prior to discovery. It is also not clear if any threat actors had accessed the data.

Following the incident Microsoft has stated that the credentials stored within the server were temporary, had been disabled, and were related to systems only accessible via the internal network. However, the data could be used to help craft future attacks if accessed by threat actors.

Wider implications

This incident highlights that accidental data exposure can pose just as significant a risk as malicious threat actors.

Cyber security is not just about preventing threat actors from exploiting vulnerabilities or carrying out social engineering attacks, but also about securely configuring an organisation's internal environment, minimising access to only those who require it.

Even if the data involved is not directly damaging to the organisation or any individuals, as it appears in this incident, it could be used to craft more sophisticated and effective attacks in the future.

Any internal-only information that is revealed could be used by threat actors to gain a better understanding of an organisations internal environment or conduct more sophisticated and targeted social engineering attack.

Stay safe out there

So you can stay up to date on all things Cyber, why not sign up to our monthly Cyber Report, where you can gain access to more insightful cyber news, like this one.

Sign up here.

If you want to learn more about how you can improve your Cyber security, take a look at our recent articleGet Breach Ready - Minimise the impact of a successful cyber attack.