Microsoft Exposes Customer Records

By Mark A. Wells

You would think that a company as tech savvy as Microsoft would always have a great handle on how they secure their databases. However, in this case Microsoft left 250 million Microsoft customer records exposed online in a database without password protection. Records including customer data, conversations with Microsoft customer service, support logs detailing conversations, and other information spanning from 2005-2019 on five unprotected servers were exposed online to anyone with the desire to access them. Davey Winder reports, “When I say unsecured, I mean that the data was accessible to anyone with a web browser who stumbled across the database: no authentication at all was required to access them. . .”[1] Although it appears much of the personally identifiable information was redacted, the database did contain customer e-mail addresses, IP addresses, geo-locations, descriptions of services rendered, support claims, support agent e-mails, case numbers, etc. which could potentially be used to scam customers through the all too common Microsoft scams solicited by fraudsters wishing to carry out cyber-attacks.

On December 28, 2019 two threat intelligence search engines, BinaryEdge and Comparitech found the databases and informed Microsoft of the issue. Comparitech security research teams notified Microsoft of the problem on December 29. Within 48 hours Microsoft had all servers secured. Clearly Microsoft recognized the severity of the leak and the potential for misuse of this information by fraudsters. It is unclear if the databases were in fact accessed by anyone during the exposure, and on January 22, 2020 Microsoft suggested that their “investigation found no malicious use.” Microsoft also determined that the exposure began December 5, 2019, just 14 days before it was discovered. Microsoft reported that the exposure was due to “misconfigured security rules, and was remedied on December 31, 2019.” The firewall rules determine who can and cannot access what from where. In this case they were allowing anyone with a web browser access to this database. This appears to be a very preventable data breach. There are mechanisms they could have put in place to detect misconfigurations of this kind.

Perhaps the biggest surprise/irony is that Microsoft, perhaps the largest vendor of online security services, allowed this exposure to happen. Since Microsoft is a multi-national company that does business nearly everywhere in the world, it comes as no surprise that this exposure is being investigated in the EU (European Union) under the General Data Protection Regulation (GDPR), which would impose hefty fines if Microsoft were found guilty.

[1] Davey Winder, “Microsoft Security Shocker As 250 Million Customer Records Exposed Online,” *Forbes*, Jan. 22, 2020.

This Careers Preparation National Center product was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-22-1-0329), which is part of the National Security Agency.

Sources:

Davey Winder, “Microsoft Security Shocker As 250 Million Customer Records Exposed Online,” Forbes, Jan. 22, 2020.

Igor Bonifacic, “Microsoft Accidentally Exposed 250 Million Customer Service Records,” *Wired*, January 22, 2020.