THSH Cyber Alert: GoDaddy the latest to leave S3 Bucket Unsecured

Businesses using Amazon Web Services and their Customers Susceptible to Breaches

A spate of incidents involving prominent businesses inadvertently leaving their data – and the data of their customers – unsecured and visible to the public has shed light on a serious risk inherent in the use of Amazon Web Services' Simple Storage Service (or S3). Last week, data from over 31,000 of GoDaddy's private and proprietary business systems and other confidential business information were exposed to the public.[1]

Described by Amazon as "a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web", S3 uses what Amazon calls "buckets" in which customers store their files.[2]

While Amazon makes both static and in-transit encryption available for the files stored in its buckets, the numerous high-profile breaches of late demonstrate that encryption or other security measures are not always activated by users (often, even ostensibly sophisticated ones).

To make matters worse, it was reported last month that a new free application is available to let users locate unsecured S3 buckets.[3]

Fortunately for companies that use Amazon Web Services, buckets can be secured. Users can manage their access settings and enable several types of encryption. Unfortunately, while users can have a degree of control over their own buckets, consumers are generally at the peril of the safekeeping (or lack thereof) employed by the multitude of third parties who hold and use their personal information.

This story is another reminder of the need to remain vigilant and informed in the face of the pervasive threat to data security in the modern age.

For any questions on this article, please contact any member of our Cybersecurity and Data Privacy practice or your regular contact at Tannenbaum Helpern.

David R. Lallouz
212.702.3142
lallouz@thsh.com

Andre R. Jaglom
212.508.6740
jaglom@thsh.com

L. Donald Prutzman
212.508.6739
prutzman@thsh.com

Michael J. Riela
212.508.6773
riela@thsh.com

[1] https://www.engadget.com/2018/08/09/amazon-aws-error-exposes-31-000-godaddy-servers/. In addition to multiple breaches since early 2017, involving proprietary and customer information by such companies as U.S. government contractor, Booz Allen Hamilton, Dow Jones & Co., Verizon, and FedEX, to name only a very few.

[2] https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html

[3] https://portswigger.net/daily-swig/a-new-tool-helps-you-find-open-amazon-s3-buckets

Beth Smigel
212.702.3176
smigel@thsh.com

Maryann C. Stallone
212.508.6741
stallone@thsh.com

Vincent J. Syracuse
212.508.6722
syracuse@thsh.com

About Tannenbaum Helpern Syracuse & Hirschtritt LLP

Since 1978, Tannenbaum Helpern Syracuse & Hirschtritt LLP has combined a powerful mix of insight, creativity, industry knowledge, senior talent and transaction proficiency to successfully guide clients through periods of challenge and opportunity. Our mission is to deliver the highest quality legal services in a practical and efficient manner, bringing to bear the judgment, common sense and expertise of well trained, business minded lawyers. Through our commitment to service and successful results, Tannenbaum Helpern continues to earn the loyalty of our clients and a reputation for excellence. For more information, visit www.thsh.com. Follow us on LinkedIn and Twitter: @THSHLAW.