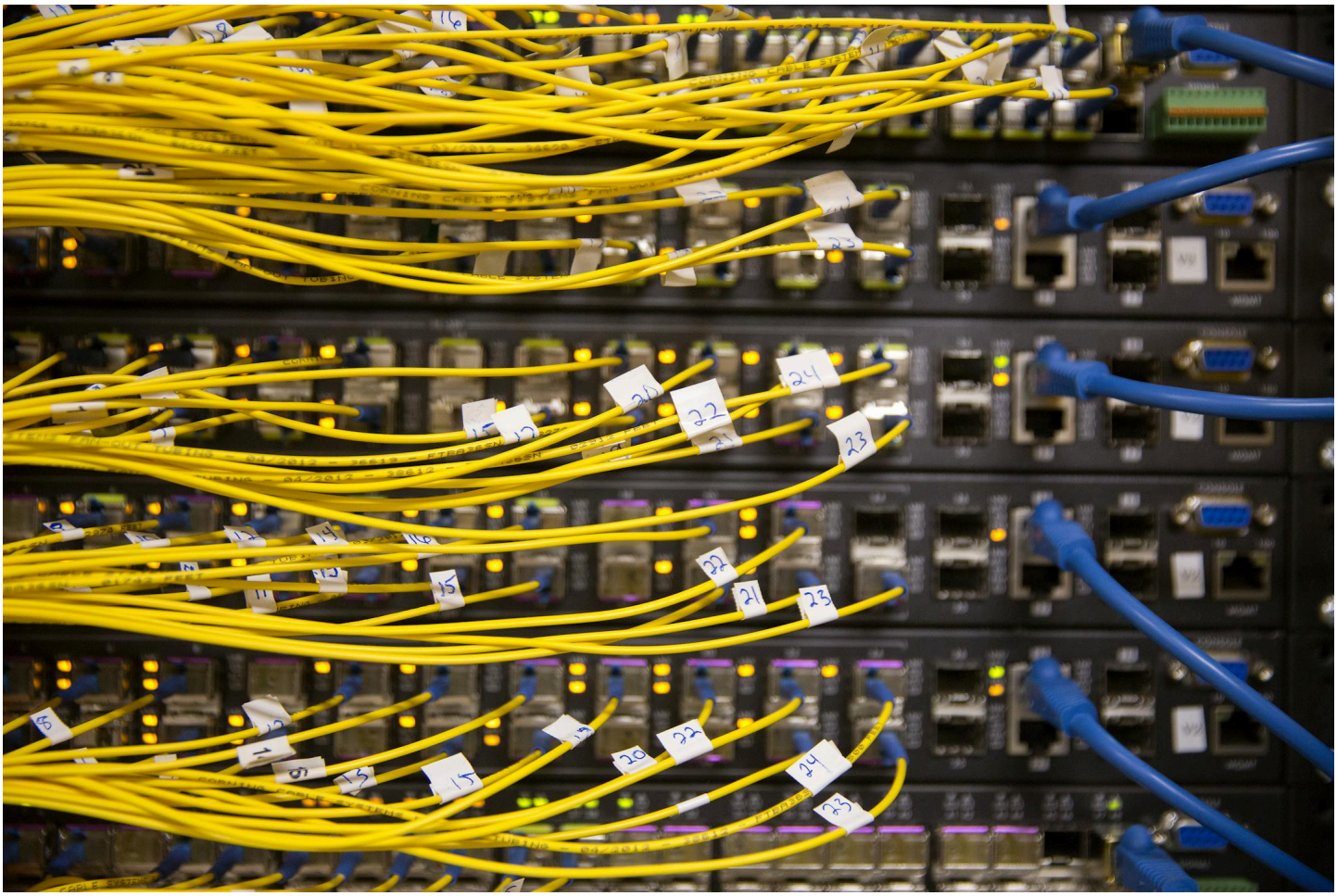
BUSINESS

Minnetonka-based US Internet's gaffe left personal email addresses exposed on webs

Thousand of emails were inadvertently publicly available, before an internet security firm spotted the flaw.

By Mike Hughlett
The Minnesota Star Tribune

FEBRUARY 15, 2024 AT 9:35PM



US Internet exposed e-mails. The company has now corrected it. Shown is a US Internet switching station. (LEILA NAVIDI/The Minnesota Star Tribune)

US Internet's email security business exposed thousands of its customers' emails on the open internet due to human error.

The gaffe was discovered by a Milwaukee computer security consultant and made public Wednesday by cybersecurity expert Brian Krebs. Minnetonka-based US Internet said Thursday the problem has been resolved, and it's assessing how much data may have been accessed.

"We were able to block it before it became a huge issue," said Travis Carter, US Internet's CEO. "It has taken a lot of work, a lot of cost and left a lot of egg on our face for lack of a better term."

US Internet generates most of its revenue by providing internet service through its own fiber-optic network in Minneapolis and adjacent suburbs. US Internet also operates an email security firm called Securence, which filters emails for spam, viruses and other threats.

The emails in question were from customers of Securence, not US Internet's general ISP business. Securence's clients include companies and governments nationwide, including in Minnesota.

Hold Security in Milwaukee discovered US Internet's vulnerability while working for its own clients.

"In some cases, we come upon systems that are in plain view" on the internet, said Alex Holden, Hold's chief information security officer.

US Internet was one of those cases. Hold discovered thousands of e-mail repositories for Securence's customers that were exposed to the public "for a long period of time," Holden said.

"The big surprise – and this is unusual – is that [Securence] is an email service provider," Holden said. "The good thing is that we found no evidence that data was stolen."

Hold Security contacted Krebs, a well-known cyber expert. Krebs' website, KrebsOnSecurity, reported that Holden and his researchers had "unearthed a public link to a US Internet email server listing more than 6,500 domain names, each with its own clickable link."

"Drilling down into those individual domain links revealed inboxes for each employee or user of these exposed host names," Krebs wrote and Carter confirmed. Some internal e-mails of current and former US Internet employees were also exposed.

"KrebsOnSecurity has been writing about data breaches for nearly two decades, but this one easily takes the cake in terms of the level of incompetence needed to make such a huge mistake unnoticed," Krebs wrote.

Before publishing his report, Krebs informed Carter of the vulnerability, and US Internet immediately wiped the information off the internet.

"The problem was a human issue," Carter said. "It was literally one command in the system."

Carter said the exposed information was on four servers, none of which host popular email services from Google and Microsoft.

As of this morning, fewer than 10 of Securence's customers – and fewer than 300 individual emails - had been accessed by unauthorized parties, he said. More than 99% of Securence's business was not affected by the error, Carter said.

Still, "I don't want to trivialize it and we are taking it very seriously."

ABOUT THE WRITER

Mike Hughlett

REPORTER

Mike Hughlett covers energy and other topics for the Minnesota Star Tribune, where he has worked since 2010. Before that he was a reporter at newspapers in Chicago, St. Paul, New Orleans and Duluth.

See More >

More from Business See More >

IN THEIR SHOES

Rural Minnesota school bus driver is a teacher as much as chauffeur