# Companies urged to use multiple vendors in wake of cyber attack

Technology

Companies can reduce the risk from the type of cyber attack that took out major websites on Friday by using multiple vendors for the critical internet service known as a domain name service, or DNS, companies and security experts said on Sunday.

" We have advocated for years for redundancy in your infrastructure," said Kyle York, chief strategy officer for Dyn, the New Hampshire DNS provider that was attacked on Friday. " I don't think you can ever be safe enough or redundant enough."

Hackers unleashed a complex attack on the internet through common devices like webcams and digital recorders and cut access to some of the world's best known websites on Friday, a stunning breach of global internet stability.

York said clients who used multiple servers " saw less of an impact."

Using multiple DNS providers can, however, make managing traffic more complicated and costly, experts said.

Friday's cyber attack alarmed security experts because it represented a new type of threat rooted in the proliferation of simple digital devices such as webcams. Such devices often lack proper security, and hackers found a way to harness millions of them to flood a target with so much traffic that it can't cope.

The attack on Dyn and the resulting outage started in the Eastern United States on Friday and then spread to other parts of the country and Europe,

affecting companies including Twitter and Paypal. DNS providers such as Dyn act as a switchboard for internet traffic.

" It's important to implement diversity geographically, as well as architecturally," for a defense against domain name service attacks, said Andy Ellis, chief security officer at Akamai Technologies, which helped Dyn recover on Friday.

Businesses can choose up to eight authoritative domain service providers, and some of the hardest-hit sites were customers who only picked Dyn.

Eliminating the threat from the unsecured devices that make up what's often called the Internet of Things will be a much tougher task, however. Many inexpensive webcams, connected thermostats, baby monitors and other products lack even basic security and sometimes use hard-coded passwords that are simple to break, security experts said.

Law enforcement authorities said on Friday they are investigating the attack. The tools making the new type of attack possible were released on the internet by unknown hackers last month, thus creating a long list of possible suspects.

" This is the new norm, the internet wasn't designed with these kinds of attacks in mind," said cyber security expert and entrepreneur Barrett Lyon.

Long term solutions would likely require governments to take far moreresponsibilityfor mandating internet security, experts agreed.

Chinese electronics component manufacturer Hangzhou XiongmaiTechnologysaid on Sunday that weak default passwords on its products inadvertently played a role in the cyber attack, according to a report from IDG News Service.

The company said it has patched the flaws and now is asking customers to change the default password the first time they use it.

(By Jilian Mincer; Additional Reporting by Joseph Menn in San Francisco and Jim Finkle in Boston; Editing by Joanthan Weber and Sandra Maler)