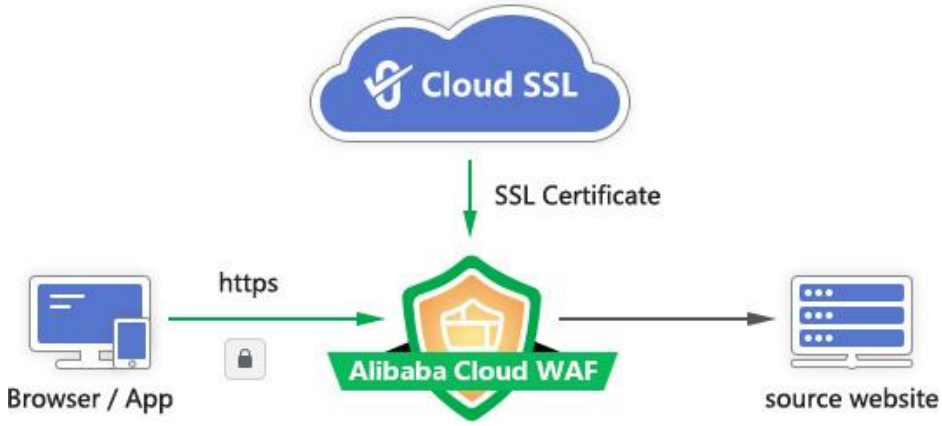
SME websites are most vulnerable to cyber attacks

The article " SMEs still an easy target for cybercriminals" published by HelpNetSecurity website on January 12, 2022, states that For SMBs, cybercrime remains a major problem, with 51% of SMBs experiencing a cyberattack, because small and medium-sized enterprises lack the resources to invest in network security like large enterprises. Among respondents who did not take cybersecurity protections, cost was the main reason for this, with 11% saying they would not spend any money on cybersecurity. 88% of businesses have at least one form of cybersecurity protection (such as antivirus, firewall, or multi-factor authentication). The consequences of experiencing a cyber-attack can be devastating for small businesses that may not be able to recover from the financial impact of a cyber-breach or lose the trust of their customers.

Although this article is a survey of Europe small and medium-sized enterprises, it is actually very suitable for the situation of small and medium-sized enterprises in China. In the current environment, it is not easy for small and medium-sized enterprises to survive. Therefore, small and medium-sized enterprises will think that "My website has nothing to steal", "My small company website will not attract the attention of hackers". In fact, hackers can use automated tools to find websites without any protection and automatically implant Trojan horses, making your website a "chicken" and a "thug" to attack other systems and passively break the law. This is the main reason why SME websites are the

most vulnerable to cyber-attacks, such as: Trojans are implanted into websites, web page tampering, SQL injection, database dragging, and email fraud etc. According to a report released by the CNCERT/CC, 53,171 websites in China were implanted with backdoors in 2020. These attacks will not only affect the normal access of websites and leak website data, but also face the pressure of compliance with the Cyber Security Law, which may receive an administrative penalty. How to do?

ZoTrus Website Security Cloud Service is a website security solution that integrates website https encryption, WAF protection and trusted identity validation. It is automatically implemented, and it supports web hosting website commonly used by small and medium-sized enterprises. It does not need to have its own independent server, does not need to install an SSL certificate or other client software on the server, and only needs to do two CNAME resolution to achieve fully automatic implementation. Trinity website security protection, in which cloud WAF protection is provided by the industry-leading Alibaba Cloud WAF.



Best of all, this trinity of website security services is affordable for small and medium-sized businesses, and can be purchased monthly, allowing you to meet Cyber Security Law compliance requirements for a small cost, without worrying about your website to be attacked, you don't have to worry that the browsers will show "Not secure", and you can do your best to do your business with confidence. This is the affordable and universal benefit security service that small and medium-sized enterprises need and affordable.

Richard Wang

June 6, 2022
In Shenzhen, China