

Whitepaper: The Importance of Web Security for SMBs

Cyber Defense Today Keeps Breaches Away

Contributors: Gabrielle Toman and Sara Talley of Data Security Solutions, LLC

“During 2015, 50% of small businesses in the United States were targets of cyber-attacks.”

February 2016 – This whitepaper discusses the importance of cyber security for small- and medium-size businesses and presents a solution.

At the start of each year, individuals and businesses alike set new goals and resolutions. Companies focus on new marketing initiatives, how to gain revenue, spend less and make more. But, what many small to medium sized businesses forget and who are most at risk, is the health of their company - Cyber Security.

During 2015, 50% of small businesses in the United States were targets of cyber-attacks.¹ In addition, generally speaking, **71% of Internet hackers target small businesses.²** These statistics are staggering in an increasingly technology-driven world. The executive chairman and former CEO of

Cisco Systems, John Chambers, stated that with “the average attack, you get 90% of the data you want in nine hours, and yet most of the companies don’t find out for three to four months.” Data breaches are not only destructive, but incredibly time sensitive. The level of damage is contingent upon the amount of time the attacker has in the company’s system. This sense of urgency is exactly what makes dotAlert® - a software application that integrates with web application firewalls (WAFs) to alert hacking attempts - so valuable in today’s market. The dotAlert security suite examines user-defined rules and configurations to instantaneously alert web administrators to active threats in real-time. When breaches are detected by the powerful Layer 7 web application firewall, the dotAlert application combines the detection and blocking of attacks by sending instantaneous email and text alerts to generate immediate action.

Ever-increasing cyber threats have created a critical need for companies to perform routine penetration tests. A *penetration test* is a controlled attempt by an organization to identify information system and website vulnerabilities, the effectiveness of the organization’s security policy and procedures, the need to implement new controls, and the importance of abiding by compliance regulations. Cash Connect, the ATM division of WSFS Bank, values the importance of threat protection and has been a user of the dotAlert security suite for over two years. “Cyber security is one of the most crucial elements of a sound technological infrastructure for any company,” says Carla Durante, Cash Connect Compliance Officer. “In order to keep the integrity of our cyber security, penetration testing is necessary to identify potential threats before

¹ <http://www.propertycasualty360.com/2015/10/07/50-of-small-businesses-have-been-the-target-of-a-c?slreturn=1454511933>

² <http://www.businessnewsdaily.com/7432-small-business-hackers.html>

they become reality.” It is important to invest in penetration testing to determine the feasibility and magnitude of possible data security breaches, and even more critical to invest in comprehensive and effective solutions.

Data security should be at the forefront of every business executive’s mind today. Unfortunately, it is not always prioritized in the company’s budget. That is why Data Security Solutions, LLC created and launched dotAlert. Allan Matyger, CTO of Data Security Solutions comments, “Many small to medium-sized businesses fall victim to cyber security attacks as a result of insufficient preparation and protection. And, a significant number of these attacks go undetected. dotAlert was created as an affordable and highly effective solution to this universal problem.” Those breaches made on smaller companies that are detected are often difficult to mitigate in a timely manner, especially without expert intervention from forensics teams and IT security specialists.

“Cyber security is one of the most crucial elements of a sound technological infrastructure for any company.”

At Cash Connect cyber security is a very serious topic. Not only is the company a dotAlert user, but it also utilizes numerous trusted vulnerability assessment in the network penetration testing industry. Just like a visit to the doctor, this helps ensure the strength and effectiveness of its security systems. Canaudit, an independent information security & IT audit consulting company based in California, provides penetration testing services to clients and comments on its website that, “our methodology includes simulations of real life attacks to uncover security gaps that can be exploited, leaving your organization at risk. Detection and response time are critical elements of our evaluation.” Canaudit performed a penetration test for Cash Connect, and noted the immediate alert technology of dotAlert software was the one of the fastest response times the company had seen.

When a company integrates dotAlert in its defense mechanism, its ability to combat website security breaches is instantaneous and real-time. dotAlert offers superior alerting technology that allows companies to respond immediately to web server threats. Companies must take proactive measures to prevent and detect hacking events with real-world effectiveness.

For more information about dotAlert:

www.dotalert.com

info@dotalert.com

[+1-405-85-ALERT](tel:+140585ALERT)

¹ <http://www.propertycasualty360.com/2015/10/07/50-of-small-businesses-have-been-the-target-of-a-c?slreturn=1454511933>

² <http://www.businessnewsdaily.com/7432-small-business-hackers.html>