SMBs Becoming Ground Zero for Cyber Crime

Comprehensive password management solutions offer safety from greatest single source of threats

WHITE PAPER

TABLE OF CONTENTS

When it comes to cybersecurity, there is a pervasive belief among many small and mid-sized businesses (SMBs) that the greatest vulnerabilities rest elsewhere—like with bigger, richer enterprise-class organizations. But there is mounting evidence that SMBs are becoming more vulnerable than their enterprise counterparts, and complacency regarding this reality can have disastrous consequences for many SMBs.

Fortunately, there are many readily accessible defenses against this rising tide of cyberthreats, not the least of which are comprehensive password management solutions that, alone, can stop an enormous number and type of attacks. In fact, comprehensive password management is a classic "no brainer" for SMBs today, given the threat environment, the relatively low expense and tremendous protection against attacks that they offer.

Just how effective is the consistent use of strong passwords in warding off common attacks? The annual Verizon Data Breach Investigations Report revealed a startling statistic: Nearly two-thirds—63%—of successful confirmed data breaches involved leveraging weak, default or stolen passwords.[1] Most, if not all, of these attacks would have been stopped by machine-generated passwords—**a feature of comprehensive password management solutions**—designed to thwart such password-related successful attacks.

[1] Verizon Data Breach Investigations Report, Verizon, 2016

Devolutions

Remote Desktop Manager

TechTarget | Custom Media

WHY SMBS ARE SUCH BIG TARGETS

That SMBs are fast becoming a huge target for cyberattacks is becoming better understood and realized. In fact, one report maintains that not only must SMBs do much more about cybersecurity, but also they must pay attention "especially (to) the password practices of their employees." The report adds that, "Despite clear evidence that the overwhelming majority of SMB cyberattacks result from poor password management, SMBs are doing very little to boost visibility into the password practices of their employees."[2]

The escalating threat to SMBs is made even more graphic by the results of the 2017 State of Cyber Security in Small & Medium Size Businesses conducted by the Ponemon Institute, which reinforced similar findings from its 2016 report.[3] The findings in the 2017 report of more than 1,000 U.S. and U.K. SMB respondents stand as a red flag for SMBs. Key findings include:

- 61% of SMBs polled reported a cyberattack, up considerably from 55% a year earlier.
- 54% reported a data breach, with employee negligence (i.e.: poor password hygiene) cited as the top root cause.
- 52% reported a ransomware attack, and stolen or compromised passwords are a leading enabler of these debilitating attacks.
- The total costs of a successful attack on an SMB now top $1 million, damages that could be ruinous for many SMBs.

PASSWORD VISIBILITY IS ESSENTIAL

A surprising number of both IT and non-IT leaders in SMBs have little or no visibility into the password practices of their own employees. In one report, the word 'password' was among the top 10 passwords used last year. Others defer to simple passwords like 123456. In fact, one study of some 13 million passwords used in data breaches showed the top five passwords in those breaches to be 123456; 123456789; 12345; 12345678; and qwerty—the consecutive letters on the top row of a conventional keyboard.

Still others share their passwords with co-workers and even third parties without a care. Many users write their passwords down on sticky notes or pads of paper that they (or anyone else for that matter) can easily access. Birthdays are very popular as passwords, too. And all too many use the same passwords or slight variations thereof to gain access to multiple systems, sites and databases.

Hackers are all too aware of these common practices in so many SMBs, which is why SMBs are fast becoming their most popular target. They represent the path of least resistance to malfeasance, the proverbial low-hanging fruit.

THE LOOMING IOT THREAT

Other escalating threats to SMB cybersecurity are less apparent, but no less dangerous. Most business leaders think of the Internet of Things (IoT)— those Internet-connected gizmos that this year will top 6.4 billion in use—as mainly applicable for consumer products. But they are very common in the SMB as programmable thermostats, smart TVs, robotic vacuums and streaming security cameras. And they have one thing in common: They arrive fresh from the factory with pre-set, very easy to hack passwords that very few individuals bother to reset.

Hacking into these devices can wreak havoc with various control systems within an SMB. In one case last year, hackers took control of 100,000 poorly secured IoT devices, then launched a botnet attack that took down Internet service for millions of customers.[4] Here again, the imposition of comprehensive password best practices would stop such attacks cold.

VALUE OF PASSWORD MANAGEMENT SOLUTIONS

Enter comprehensive password management solutions that, while not a panacea for all SMB cyberthreats, certainly do offer a very strong bulwark against the most common attack vectors and the password weaknesses they typically exploit.

Immediately, these systems give IT administrators very broad visibility into the password practices of all employees, as well as all company and personal mobile devices they are using. But even the administrators never have knowledge of the actual passwords in use. What they can determine, however, is whether the users are following prescribed password hygiene, including the use of complex passwords; not using the same password over and over, and other best practices.

The passwords generated by the system are highly complex, consisting of letters, characters and numbers. This makes them difficult, if not impossible, to break. They are also difficult, if not impossible, for users to remember. That is not a problem, however, as each user needs to remember just one password that then allows the password management system to apply its unique passwords in a highly secure manner.

[2] Why small and mid-sized businesses are a huge target for cyber attacks CSO from IDG, October 2017

[3] 2016 State of Cyber Security in Small & Medium Size Businesses, Ponemon Institute, June 2016

[4] DDoS attack on Dyn came from 100,000 infected devices, Computerworld, October 2016

And, in fact, no one at the vendor providing the password management solution has any way of accessing these machine-generated, stored passwords either. That is because the passwords, and other information a customer may wish to store, such as all credentials and other sensitive files, are kept in a highly secure data vault. An authorized user getting access to what he or she has stored in the vault is as simple as logging into it. With the so-called zero-knowledge vaults of many password management solutions, no one at the vendor can obtain access to any passwords or keys to get at that data, nor can they decrypt the data within the vaults.

PASSWORD MANAGEMENT SOLUTION WISH LIST

In seeking the best password management solution, be certain the solution in question allows for the secure creation, sharing and management of records and encrypted files across various internal teams, and possibly with third parties too. A solution with configurable policies and permissions can help harmonize the solution with other existing internal security policies and controls.

Another plus is the ability to tie the password solution to policies and procedures affecting privileged accounts and account credentials. Finally, be sure the solution offers highly secure, encrypted password management as well as a truly user-friendly interface that is available to the widest variety of operating systems and devices. It helps, as well, for compliance efforts if the solution has broad audit capabilities.

SMB LEADERS: DON'T PASS THE BUCK ON PASSWORD MANAGEMENT

One other key point regarding password management deserves some attention. Without question, the senior leadership team at a multibillion-dollar enterprise can well afford to leave password management to others, often the CIO. But the leadership at a typical SMB today can ill afford that luxury. In fact, the mantra coming from leadership at an SMB today ought to be "password management is much more than an IT problem."

In its annual Global Economic Crime Survey, PwC maintains that far too often non-IT leaders are very willing to abrogate responsibility for cybersecurity in general—of which password management is a key element— to IT. PwC then chides those organizations and leaders that do this, saying that virtually all aspects of cybersecurity, including password management, "must be embedded within an organization's culture." The report states further that non-IT leaders must "incorporate cybersecurity into their routine risk assessments and then communicate that plan up, down and across organizational lines."[5]

In other words, the importance of password management and good password hygiene starts at the top, or it may not start well at all.

[5] Global Economic Crime Survey, PwC, 2016

INDUSTRY-LEADING PASSWORD MANAGEMENT SOLUTION

A leading provider and recognized leader in remote connection, password and credential management targeting sysadmins and IT professionals, Devolutions offers a comprehensive password management system that reduces unauthorized access to vital digital assets while thwarting insider attacks as well.

Devolutions takes great care in helping clients find that critical line between true security and user accessibility to business-critical data. Devolutions accomplishes this in part by securing privileged passwords for users and administrators alike in an encrypted and hardened vault while maintaining a productive user experience.

Download a free trial version of this mission-critical solution for SMBs here.