SELF-ASSESSMENT
SCORECARD

NetDiligence Common Vulnerabilities and Exposures (CVE) Survey for Sompo International

Company name: Sompo International
Invitation sent to: Lion's Share
Submitted on: 06/26/2018 12:05 PM

In its annual Data Breach Investigation Report (DBIR), Verizon identifies the 'Top 10' Common Vulnerabilities and Exposures (CVEs) that together contribute to almost 97% of all data breaches.

Because a relatively small number of exposures creates such significant cyber risk, Sompo International has partnered with NetDiligence® to provide you with a simple way to confirm that your organization has addressed these critical vulnerabilities.
The "NetDiligence Common Vulnerabilities and Exposures (CVE) Survey for Sompo International" is an easy-to-use online survey that enables you (or your IT provider) to self-attest that certain safeguards to leading CVEs are in place. Once you have completed the survey, QuietAudit® instantaneously processes your answers and presents you with a scorecard report that benchmarks your security readiness posture for each of key CVEs and compares your scores to that of your peers.

The survey encompasses both Verizon's 'Top 10' CVEs and additional vulnerabilities documented in the National Security Federally Funded Research and Development Center's ("National Security FFRDC") published database of Common Vulnerabilities and Exposures (CVE). The CVE database is used by software solutions vendors and organizational IT managers alike to recognize and address known security weaknesses that may be inherent in their deployed systems and applications. The top CVEs included in this technical survey are organized into six (6) categories:

1. Network Monitoring Security
2. Terminal Services Security
3. TLS/SSL Security
4. Network Services Security
5. Web Scripting Security
6. Legacy Operating System (OS) Security

This online survey should be completed by your organization's Chief Information Security Officer or organizational equivalent and takes approximately 40 minutes to complete.

This CVE Survey is based upon a limited (sampling) survey of network risk factors and industry recognized best and baseline practices associated with information and network security and related processes. By offering this service, NetDiligence does NOT make any representations about the actual or potential risk exposures associated with the customer.

Report Card Calculation Methodology

This report card is intended to highlight your organizations' overall score on the CVE Survey. The total possible score is 100% for each section, and for the cumulative average of all sections combined. This report card may indicate areas of improvement for your Network Security and Risk Management Program. For specifics on which areas or questions you scored high and low on, please review the survey and your answers. "No" or "In Progress" responses may indicate likely areas for improvement.

	Section	Summary	Scores		Issues
1	Network Monitoring Security Network monitoring allows an organization to track and manage the availability and capacity of IT assets on the network. Such monitoring usually makes extensive use of the Simple Network Management Protocol (SNMP) service to collect this information for processing and display. The information provided through SNMP can also be used by malicious individuals to gain unauthorized access to systems and sensitive information. As a result, all organizations should take care to keep SNMP services up-to-date and configured for maximum practical security.	Ok	Your score Others	88.8% 61.3%	N/A
2	Terminal Services Security Remote terminal services, if not configured securely and kept up-to-date, can provide malicious individuals with	Weak	Your score Others	51.3% 72.8%	Issue

	Section	Summary	Scores	Issues
	opportunities to gain unauthorized access to systems and information through eavesdropping and/or session hijacking. To minimize the probability of such an occurrence, organizations should configure terminal services such that connectivity is limited only to authorized individuals and such that sensitive information cannot be viewed in transit by unauthorized third parties.			
3	TLS/SSL Security The Transport Layer Security (TLS) protocol (formerly known as Secure Sockets Layer, or SSL) is primarily utilized to secure information flowing between Web servers and browsers. Many encryption and hashing algorithms historically used by TLS (and older SSL) have been shown to have security weaknesses and vulnerabilities. Because the information traveling between Web servers and browsers is often of a sensitive nature, any organization making use of TLS for user authorization and/or data confidentiality must keep their TLS services up-to-date and configured for maximum practical security.	Ok	Your score 85% Others 84%	N/A
4	Network Services Security Any network service can have vulnerabilities that can be exploited by malicious individuals to gain unauthorized access to IT resources and sensitive information. Accordingly, all security-sensitive organizations should implement network controls to limit access to such services as well as review such services for upgrade and/or deactivation when they are no longer needed. When access to sensitive information is facilitated by such services, network controls should be configured to encrypt that information as it travels between the service and the end user or information consumer.	Ok	Your score 85% Others 84%	N/A
5	Web Scripting Security The extensive feature set that is provided by most Web servers (e.g. support for dynamically-generated content) typically exposes a larger attack surface to the outside world than is associated with other network services. Accordingly, it is important to configure all Web servers for maximum practical security, to review all programs running under the control of Web servers, and to implement such programs that minimize or eliminate the introduction of new vulnerabilities.	Ok	Your score 70% Others 79%	N/A
6	Legacy OS Security Older versions of operating systems have greater numbers of well-known vulnerabilities. As a result, they present a major source of risk to any organization. To limit these risks, such operating systems should be kept updated with security patches to the greatest extent possible and should have security software installed that provides protection for all forms of malware. At the earliest practical opportunity, services utilizing legacy operating systems should be transitioned to newer operating systems whenever possible.	Ok	Your score 73.8% Others 78.8%	Issue
	Score Average and Total Issue Sections		Your score 75.7% Others 76.7%	

Summary terminology

OK	The responses to the applicable questions in the survey indicate that most or all of the best practices are observed. Where "OK" appears with a green light, the company achieved 75% or more of the applicable points within a given section.
OK	The responses to the applicable questions in the survey indicate that most or all of the best practices are observed. Where "OK" appears with a yellow light indicates the company achieved a marginal passing score 60%.
Weak	The responses to the applicable questions in the survey indicate that best practices are not being followed and that significant vulnerabilities may exist. The company achieved less than 60% of the applicable points for a given section.

Issue terminology

N/A	No issues-based questions have been designated in this section that reflect critical requirements or address a baseline control.
Issue	The responses to the applicable questions in the survey indicate that while best practices are observed in some or most cases, inattention to certain critical requirements exist and immediate attention toward these items may be necessary. Regardless of the score achieved by the company for a given section, responses to one or more key questions indicated a specific weakness that must be addressed immediately.
No issue	No issues have been found.