Parasol Island

Arbeitsanweisung zur Netzwerkeinrichtung

Dateiname:	03_09_PSL_ISMS_Netzwerkeinrichtung_v00.10_pN
Dokumentenebene:	03_Arbeitsanweisung
Erstellt von:	Justus Heinser
Version:	00.10
Status:	Freigegeben
Letzte Aktualisierung am/von:	10.11.2017 | Peter Norenkemper
Exportiert am:	10.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	10.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	-

Version	Datum	Autor	Änderung
00.01	30.08.2017	Justus Heinser	Erstellung
00.02	19.09.2017	Justus Heinser	Anpassungen
00.03	17.10.17	Cedric Wolffs	Anpassung der Serverstruktur
00.04	07.11.17	Cedric Wolffs	Ergänzungen Firewall und Server
00.10	10.11.17	Peter Norenkemper	Finalisierung

Parasol Island

Inhaltsverzeichnis

Parasol Island

1. Ziel der Handlungsanweisungen für ausgewählte Schadensereignisse

Die Arbeitsanweisung für Netzwerkeinrichtung soll die Struktur und Konfiguration des Parasol Island Netzwerkes dokumentieren und helfen, Sicherheitslücken zu diagnostizieren, sowie im Falle eines Schadensereignisses die Einrichtung wieder zu rekonstruieren.

2. Firewall Konfiguration

Die Sophos SG210 Firewall erlaubt einen qualitativ hochwertigen Schutz des Intranets.

Features wie Anti-Virus und IDS (Intrusion Detektion Prävention), welche vom Hersteller Sophos regelmäßig und automatisch mit neuen Signaturen versorgt werden, sorgen für einen effektiven Schutz des Netzwerkes und für eine schnelle Erkennung von Bedrohungen.

Interface Einstellungen:

Wan 1 (Händle & Korte)

185.6.68.160/27

Wan 2 (QSC)

87.193.232.112/29
83.236.171.192/29

Wan 3 (Unitymedia)

130.180.99.168/30

Lan 1

192.168.0.0/24

VLan 1 (Server)

10.100.0.0/16

VLan 2 (Client)

10.110.0.0/16

VLan 3 (DMZ)

10.190.0.0/16

WLan 1 (Private)

10.20.0.0/16

WLan 2 (Public)

10.30.0.0/16

DNS Server

10.100.1.1
10.100.1.2

Das Gerät ist bei Sophos zu registrieren und mit einer jährlich zu erneuern Lizenz für die Update Dienste auszustatten. Täglich wird auf Sicherheitsupdates geprüft und per Mail darüber informiert.

Die Lizenz ist vor dem Auslaufen zu erneuern, um keine Lücken im Schutz aufkommen zu lassen.

Regeln für Dienste wie AV und IDP sind zu erstellen und zu aktivieren. Die voreingestellten Presets sind dafür ausreichend.

3. Wireless LAN

Mobile Arbeitsgeräte

Für Mobile Arbeitsgeräte wird sowohl im Nord- als auch im Südteil des Büros ein Wireless LAN (ParasolPrivate) ausgesendet, welches direkten Zugang zum Firmennetzwerk hat. Der Zugriff auf Dateien erfordert zusätzlich eine offizielle Authentifizierung, welche von der Geschäftsleitung autorisiert und vom Administrator eingerichtet werden muss. Der Wireless LAN Zugang ist ausschließlich für firmeneigene Geräte und die Zugangsdaten können beim Administrator erfragt werden.

Kunden

Für Kunden steht ein eigenes Wireless LAN (ParasolPublic) im Nord- als auch im Südteil des Büros zur Verfügung dieses ist über die Firewall physikalisch vom sicheren Netzwerk getrennt und liefert ausschließlich einen Internetzugang.

4. Server

pslsrv10 / pslsrv17

Datenserver mit Projektdateien

psldc01 / psldc02 / psldc03

Domaincontroller

pslsrv05

Server für das Kopieren von Backups und Archivierungen

Licenser (pslsrv24 / pslsrv25 / pslsrv09 / pslsrv11)

Server zur Verwaltung von Lizenzen

5. Trennung von Produktions- und Management-Netzwerken

Durch die Anpassung der Netzwerkstruktur ist die Trennung von Management-Netzwerk und Produktions-Netzwerk umgesetzt worden. Dies wird mit der Nutzung von VLAN (Virtual Local Area Network) zur logischen Trennung beider Netze sichergestellt.

Folgende Komponenten werden über das Management-Netzwerk angesteuert:

Switches:

Die Management-Ports der Switches werden auf einen Port im VLAN gepatched.

Firewall:

Die Firewall ist so konfiguriert, dass nur von dem getrennten LAN-Port, welcher auf einen VLAN-Port im Switch gepatched, ist auf das Webinterface zugegriffen werden kann.

Wireless Access Points:

Wireless Access Points bieten über nativen VLAN-Support die Möglichkeit, Management-Funktionen wie das Webinterface nur über ein spezifiziertes VLAN bereitzustellen.

Die Wireless Access Points werden über speziell konfigurierte VLAN-Ports am Switch angeschlossen.

Zugang zum Management-Netz besteht nur vom Arbeitsplatz des Administrators über eine getrennte Netzwerkleitung und über einen designierten freien Port am VLAN-Switch.

(VDA ISA 13.1)

6. Netzwerkdiagramm