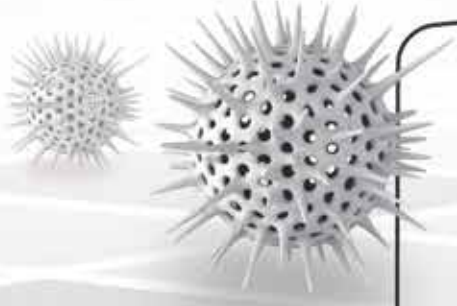
SECURITY CHECKUP

THREAT-ANALYSE REPORT

Erstellt für:	ABC Corp.
Erstellt von:	Check Point Solution Center und Westcon Security
Datum:	20. Januar 2014
Dokument-Version:	2.0



Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

INHALTSVERZEICHNIS

EXECUTIVE SUMMARY

Dieses Dokument stellt die Ergebnisse einer kürzlich durchgeführten Security-Analyse Ihrer Infrastruktur dar. Es gibt Ihnen sowohl eine Zusammenfassung der Untersuchungsresultate als auch Empfehlungen für die Adressierung aufgedeckter Sicherheitsprobleme an die Hand.

Die Analyse basiert auf der Sammlung von Daten unter Berücksichtigung nachstehender Charakteristika:

Security Analysis Date:	12/01/2014	**Dauer der Analyse:**	2 Wochen
Industrie:	Versicherungsbranche	**Land**	USA
Unternehmensgröße:	2.500 EMitarbeiter	**Analysiertes Netzwerk**	Internes LAN
Security Gateway-Version:	R77	**Analyse-Modus:**	Mirror Port
Security Gateway Software Blades:	Application Control, URL Filtering, Anti-Bot, Anti-Virus, IPS, DLP, Identity Awareness , Threat Emulation, Compliance		
Security-Device:	Check Point 4800 Security Gateway		

Nachstehend finden Sie eine Übersicht über die häufigsten und risikoreichsten Security-Events, die im Rahmen dieser Analyse aufgedeckt wurden

ZUGRIFFSKONTROLLE & DATENSCHUTZ

30.670	hoch riskante Application-Events
22	Data Loss-Events

THREAT PREVENTION

9	Bot-Events
5	Virus-Events
16	Zero-day-Events
18	Intrusions- & Attacks-Events

ENDPOINT

893	Endpoints, die in hoch riskante Events involviert sind

COMPLIANCE

65%	compliant with Check Point Best Practices
58%	compliant mit behördlich angeordneten Bestimmungen

01 ERGEBNISSE IM BEREICH ZUGRIFFS-KONTROLLE & DATENSCHUTZ

WEB SECURITY-EVENTS

Die risikoreichsten Applikationen & Sites

In den Bereichen Web-Applikationen und Websites weisen nachstehende Elemente die höchsten Risiken[1] aus:

Application / Site	Category	App Risk	Number of Users	Traffic	Number of Events
Tor	Anonymizer	5 Critical	35	149 MB	228
Ultrasurf	Anonymizer	5 Critical	33	1 GB	51
Coralcdn	Anonymizer	5 Critical	2	2 MB	45
VTunnel	Anonymizer	5 Critical	1	24 MB	18
Kugou	P2P File Sharing	5 Critical	2	7 MB	15
Suresome	Anonymizer	5 Critical	7	1 MB	9
Hola	Anonymizer	5 Critical	3	98 KB	4
PacketiX VPN	Anonymizer	5 Critical	2	300 KB	2
Kproxy	Anonymizer	5 Critical	1	400 KB	2
Sopcast	P2P File Sharing	5 Critical	1	350 KB	1
DarkComet-RAT	Remote Administration	5 Critical	1	260 KB	1
Dropbox	File Storage and Sharing	4 Critical	3573	37 GB	19,443
GoToAssist-RemoteSupport	Remote Administration	4 Critical	1573	4 GB	5,733
Lync	Instant Messaging	4 Critical	118	937 MB	1,144
TeamViewer	Remote Administration	4 Critical	182	831 MB	768
BitTorrent Protocol	P2P File Sharing	4 Critical	113	168 MB	464
Lync-sharing	Instant Messaging	4 Critical	93	70 MB	443
uTorrent	P2P File Sharing	4 Critical	2	21 MB	327
QQ IM	Instant Messaging	4 Critical	30	26 MB	294
Free Download Manager	Download Manager	4 Critical	6	373 MB	257
AOL Desktop	Anonymizer	4 Critical	47	2 MB	233
ad.adlegent.com/iframe	Spam	4 Critical	3	32 MB	228
linkuryjs.info	Spam	4 Critical	2	85 MB	227
Dropbox-web download	File Storage and Sharing	4 Critical	2	3 MB	193
LogMeIn	Remote Administration	4 Critical	39	30 MB	179
digsby	Instant Messaging	4 Critical	36	5 MB	166
ZumoDrive	File Storage and Sharing	4 Critical	17	3 MB	148
AliWangWang	File Storage and Sharing	4 Critical	2	3 MB	140

[1] Risiko-Level 5 indiziert eine Applikation, die die Security umgehen oder Identitäten verbergen kann (z. B.: Tor, VTunnel). Risiko-Level 4 indiziert eine Applikation, die ohne Wissen des Anwenders zu Datenlecks oder Malware-Infektionen führen kann (z.B.: File Sharing, P2P uTorrent oder P2P Kazaa). Applikationen für die Remote-Administration sind möglicherweise, sofern sie von Admins und Helpdesk genutzt werden, legitimiert.

Hoch riskante Applikationen, die compliant mit der organisatorischen Security Policy sind

Hoch riskante Applikationen sind Anwendungen, die ohne Wissen des Anwenders die Security umgehen, Identitäten verbergen und Datenlecks oder sogar Malware-Infektionen verursachen können. In den meisten Fällen ist die Nutzung solcher Applikationen nicht vereinbar mit der Security Policy des Unternehmens. In einigen Fällen können jedoch spezifische Applikationen mit der organisatorischen Policy compliant gemacht werden. Nachstehende, sehr risikoreiche Applikationen wurden während der Analyse entdeckt, gehen jedoch konform mit der bestehenden Security Policy:

Application	Organisatorische Security Policy
TeamViewer	Zugelassen für die Nutzung durch Support-Teams bei der Remote-Unterstützung der Kunden
LogMeIn	Zugelassen für die Nutzung durch den Helpdesk bei der Remote-Unterstützung von Mitarbeitern

Beschreibung der risikoreichsten Applikationen

Die nachstehende Tabelle ist eine zusammenfassende Erläuterung der gefunden Top-Events und der damit verbundenen Security- oder Geschäftsrisiken:

Applikation und Beschreibung	Kategorie	App.-Risiko	Events
Tor Tor ist eine Applikation, die Online-Anonymität ermöglichen soll. Die Tor-Client-Software leitet Internet-Traffic durch ein weltweites, hierfür frei zur Verfügung gestelltes Netzwerk von Servern, um so bei der Durchführung von Netzwerk-Monitoring oder Traffic-Analysen den Standort und die Nutzungsgewohnheiten von Anwendern zu verbergen. Die Nutzung von Tor erschwert die Rückverfolgung von Internetaktivitäten wie Website-Aufrufen, Online-Posts, Instant Messages und anderen Kommunikationsformen zum Anwender.	Anonymizer	Kritisch	228
Ultrasurf Ultrasurf ist ein freies Proxy-Tool, das Anwendern das Umgehen von Firewalls und Software für das Blockieren von Internet-Content ermöglicht.	Anonymizer	Kritisch	51
VTunnel VTunnel ist ein frei erhältliches, anonymes Common Gateway Interface (CGI)-Proxy, das IP-Adressen verdeckt und dem Anwender das anonyme Aufrufen und Anschauen von Websites sowie das Umgehen von Sicherheitsmaßnahmen für die Netzwerk-Security ermöglichen.	Anonymizer	Kritisch	18
BitTorrent BitTorrent ist ein Peer-to-Peer File Sharing-Kommunikationsprotokoll und eine spezifische Methode für die weite Verbreitung von großen Datenmengen. Es existiert eine Vielzahl kompatibler BitTorrent-Clients, die in unterschiedlichen Programmiersprachen erstellt und auf einer Vielzahl von Plattformen lauffähig sind. P2P-Applikationen können, ohne dass es der Anwender bemerkt, zu Datenlecks oder Malware-Infektionen führen.	P2P File Sharing	Hoch	464
ZumoDrive ZumoDrive ist eine hybride Cloud Storage-Applikation. Sie ermöglicht Anwendern den Zugriff auf ihre Musik, Fotos und Dokumente über Computer und Mobiltelefone. Daten-Sharing in einer öffentlichen Cloud kann zum Verlust von sensitiven Daten führen.	File Storage und Sharing	Hoch	148

Anwender, die hoch riskante Applikationen am häufigsten nutzen

Nachstehende Anwender waren in die am häufigsten auftretenden Events mit riskanter Applikations- und Web-Nutzung involviert:

Anwender	Events
Ginger Cash	12
Ivan Whitewash	9
Jim Josh	7
Bob Bash	5
Damien Dash	2

***Anmerkung**: Benutzernamen werden in der oben stehenden Tabelle nur dann dargestellt, wenn das Check Point Identity Awareness Software Blade aktiviert und konfiguriert ist.

DATA LOSS-EVENTS

Ihre Geschäftsdaten gehören zu den wertvollsten Gütern Ihrer Organisation. Jede Form von Datenverlust, ob geplant oder unbeabsichtigt, kann Ihrem Unternehmen Schaden zufügen. Nachstehend haben wir die Charakteristika der Vorkommnisse von Datenverlust aufgelistet, die während der Durchführung unserer Analyse identifiziert wurden.

Die gravierendsten Ereignisse von Datenverlust

Die nachstehende Liste fasst die identifizierte Datenverlust-Aktivität und die Häufigkeit, mit der spezifische Typen von Datenverlust auftraten, zusammen.

Schweregrad	Daten	Kategorie	Events
Kritisch	Kreditkartennummern	Compliance-Vorschrift	5
Hoch	Business-Plan	Geschäftsinformation	6
	Finanzberichte	Finanzinformation	3
	Source Code	Geistiges Eigentum	2
	Outlook-Nachricht, vertraulich	Vertrauliche Information	1
Medium	Lohnabrechnung	Personalabteilung	4
	US-Sozialversicherungsnummern	Personenidentifikationsinformation	1

Wichtige Dateien, die das Unternehmen über HTTP verlassen haben

Nachstehende Tabelle listet Dateien auf, die aus dem Unternehmen heraus gesendet wurden und sensitive Daten enthalten können.

Host	Datentyp	Dateiname	URL
192.168.75.26	Kreditkartennummern	customer orders.xlsx	www.ccvalidator.com
192.168.75.48	Finanzberichte	Q4 Report - draft2.docx	www.dropbox.com
192.168.125.28	Source Code	new_feature.C	www.java-help.com
192.168.125.10	Kundennamen	Customer List.xlsx	www.linkedin.com
192.168.125.78	HIPAA – Geschützte Gesundheitsinformation	Medical File - Rachel Smith.pdf	www.healthforum.com

Wichtige Dateien, die das Unternehmen über SMTP verlassen haben

Nachstehende Tabelle listet Dateien auf, die aus dem Unternehmen heraus gesendet wurden und sensitive Daten enthalten können.

Empfänger	Datentyp	Dateiname	Email-Betreff
bella@otherBiz.com	Kreditkartennummern	Customer Invoices.xlsx	FW: Rechnungen
betty@otherBiz.com	Business-Plan	Q1 2015 Goals.pdf	RE: 2015 Plan
doreen@otherBiz.com	Namen von Mitarbeitern	employees.xls	Mitarbeiter
zoe@otherBiz.com	Sales Force-Reports	Q4 sales summary.doc	RE: Q4 Sales. Vertraulich!
jordana@otherBiz.com	Pressemitteilung des Unternehmens	New Release - draft2. docx	FW: Neues Release PR Entwurf - nicht weiter leiten!!

Die wichtigsten Ereignisse von Datenverlust nach Email-Absender

Diese Tabelle zeigt den Verlust von Daten nach Email-Absender in Ihrem Netzwerk auf.

Absender	Events
tommythrash@myBiz.com	4
susansash@myBiz.com	4
joejosh@myBiz.com	4
ikewhitewash@myBiz.com	3
johnjosh@myBiz.com	3
ebenezereyelash@myBiz.com	2
jeffjosh@myBiz.com	2
claudecash@myBiz.com	1
bradbash@myBiz.com	1
chloecash@myBiz.com	1

02 ERGEBNISSE IM BEREICH THREAT PREVENTATION

BOT EVENTS

Ein Bot ist eine Schadsoftware, die in Ihren Computer eindringt. Sie ermöglicht kriminell motivierten Angreifern ohne Wissen der Anwender die Fernkontrolle über deren Computersysteme zu übernehmen und diese für illegale Aktivitäten zu missbrauchen, wie z.B. den Diebstahl von Daten, die Verbreitung von Spam und Malware, die Beteiligung an Denial of Service-Attacken u.v.m.

Bots werden oft als Werkzeuge für s.g. Advanced Persistent Threats (APTs)-Attacken genutzt. Ein Botnet ist eine Sammlung solcher, kompromittierter Computersysteme.

Die nachstehende Tabelle zeigt die mit Bots infizierten Hosts und deren Aktivitäten auf, die in Ihrem Netzwerk identifiziert wurden.

Mit Bots infizierte Hosts	8
Hosts mit installierter Adware	1
Hosts mit SMTP- und DNS Malware-verbundenen Events	2

Schadhafte Bot-Aktivitäten

Beschreibung	Häufigkeit
Bot-Kommunikation mit C&C-Site	4
Bot-Testverbindung	2
Andere schadhafte Aktivität durch Bot-Infektion	1
Unerwünschte Netzwerkaktivität durch installierte Adware	1
Events gesamt	**8**

Hosts mit hoher und kritischer Bot-Aktivität

Während der Durchführung des Security Check-Ups identifizierte die Check Point-Lösung eine Anzahl Malware-bedingter Events, die auf Bot-Aktivitäten schließen lassen. Diese Tabelle listet einige Beispiele von Hosts auf, die besonders hohen Risiken ausgesetzt waren.

Host	Aktivität	Name der Gefährdung	Quelle
192.168.75.7	Kommunikation mit C&C	Operator.Virus.Win32.Sality.d.dm	yavuztuncil.ya.funpic.de/images/logos.gif?f58891=16091281
10.10.2.32	DNS Client-Anfrage oder DNS Server löst in eine C&C-Site auf	Operator.Conficker.bhvl	zsgnmngn.net
192.168.75.22	DNS Client-Anfrage oder DNS Server C&C-Site	Operator.Zeus.bt	zsxwd.com
172.23.25.35	DNS Client-Anfrage oder DNS Server C&C-Site	Operator.BelittledCardigan.u	zwoppfqnjj.com
10.100.2.33	DNS Client-Anfrage oder DNS Server C&C-Site	Operator.APT1.cji	zychpupeydq.biz
10.1.1.22	DNS Client-Anfrage oder DNS Server C&C-Site	Operator.Virus.Win32.Sality.f.h	zykehk.com

Weitere Details über die im Rahmen dieses Reports identifizierte Malware finden Sie im Check Point ThreatWiki, Check Points frei verfügbarer Malware-Datenbank, unter **threatwiki.checkpoint.com**

VIRUS EVENTS

Cyberkriminelle nutzen verschiedene Kanäle für die Verbreitung von Malware. Zu den gängigsten Methoden gehört es, den Anwender zum Öffnen einer infizierten Datei im E-Mail-Anhang zu animieren, schadhafte Files herunterzuladen oder auf einen Link zu klicken, der auf eine schadhafte Website führt.

Nachstehende Tabellen fassen die in Ihrem Netzwerk festgestellten Vorfälle von Malware-Downloads und Zugriffen auf infizierte Websites zusammen.

Malware Downloads

Beschreibung	Ergebnisse
Hosts haben Schadsoftware heruntergeladen	8
Anzahl der entdeckten Events	9

Zugriff auf schadhafte Webseiten

Beschreibung	Ergebnisse
Hosts haben auf eine bekanntlich mit Malware infizierte Seite zugegriffen	5
Anzahl der entdeckten Events	8

Hosts mit häufigen und kritischen Virus-Events

Im Laufe der Security-Analyse identifizierte die Check Point-Lösung einige mit Malware im Zusammenhang stehende Events, die auf das Herunterladen schadhafter Dateien oder Verbindungen zu Malware-infizierten Seiten hinweisen.

Folgende Tabelle zeigt einige Beispiele von Hosts, die besonders risikoreichen Events ausgesetzt waren.

Host	Aktivität	Quelle
192.168.75.78	Download eines schadhaften Files/ Exploits	r.openx.net/set?pid=619cb264-acb9-5a18-89ed-c1503429c217&rtb=3105223559/basic.pdf
192.168.125.76	Download eines schadhaften Files/ Exploits	lavilla.de/links.jpg
192.168.125.10	Zugriff auf bekanntlich schadhafte Website	zzoygsulaeli.com/img_cache.php
192.168.125.48	DNS Server bereinigt eine Seite, die bekanntlich Malware für einen dahinter stehenden Client enthält	zzoygsulaeli.com

Weitere Details über die im Rahmen dieses Reports identifizierte Malware finden Sie im Check Point ThreatWiki, Check Points frei verfügbarer Malware-Datenbank, unter **threatwiki.checkpoint.com**

ZERO DAY-GEFÄHRDUNGEN

Im Zuge sehr ausgefeilter und immer raffinierterer Cyber-Attacken werden nahezu täglich neue Exploits verbreitet, gegen die es noch keine Schutzmaßnahmen gibt. Dazu gehören vor allem Zero-day-Attacken auf neue Schwachstellen sowie zahllose, neue Malware-Varianten.

Dieser Abschnitt fasst die in Ihrem Netzwerk festgestellten Zero-day-Gefährdungen zusammen. Für eine detaillierte Malware-Analyse zu einem spezifischen Event kontaktieren Sie bitte den für diesen Report zuständigen Check Point-Repräsentanten.

Anzahl untersuchter Dateien	**169**

Event	**Ergebnisse**	**Involvierte Hosts**
Aus dem Web heruntergeladene Zero-day-Malware	7	6
Per E-Mail (SMTP) verschickte Zero-day-Malware	9	9

Häufigste, aus dem Web heruntergeladene Zero-day-Malware

Datei	Malware-Aktivität	Host	Quelle
0dd730ed4.pdf	Unerwarteter Prozessabbruch/ Crash	192.87.2.7	www.lostartofbeingadame.com/ wpcontent/plugins/ www.fotosupload.php
guide04d88.pdf	Schadhafte Dateisystemaktivität Schadhafte Netzwerkaktivität Schadhafte Verzeichnisaktivität Unerwartete Prozess-Erzeugung Unerwartete Prozess-Beendigung	10.23.33.24	silurian.cn/modules/mod_cmsfix/ fix.php

Häufigste, per Email (SMTP) verschickte Zero-day-Malware

Datei	Sender	Empfänger	Betreff	Malware-Aktivität
Notice231488.doc	asia@ shippingoods.com	logistics@ mybiz.biz	Versandinfor-mationen	Malware erzeugt einen weiteren Prozess Malware erzeugt verdächtige Dateien Malware fragt Modul-Namen ab Malware vermehrt sich selbst Malware verändert den Browserverlauf
invoiceBQW8OY.doc	No-Replay@ shop.sip	jhon@ mybiz.biz	Ihre Rechnung	Malware schädigt einen anderen Prozess auf dem System Malware erzeugt einen weiteren Prozess Malware erzeugt verdächtige Dateien Malware erzeugt einen Suspended Status (um einen Prozess zu umgehen) Malware löscht sich selbst Malware fragt Modul-Namen ab Malware läuft im Kontext eines anderen Prozesses Malware erzeugt einen Child Process Malware verfälscht Browserverlauf
Summit_Agenda.doc	events@ conferences.org	marketing@ mybiz.biz	Agenda für die anstehende Veranstaltung	Malware erzeugt einen weiteren Prozess Malware erzeugt verdächtige Dateien Malware erzeugt einen Suspended Status (um einen Prozess zu umgehen) Malware löscht sich selbst Malware fragt Modul-Namen ab Malware verändert wichtige Systemdateien

INTRUSION- & ATTACK-EVENTS

Die häufigsten Intrusion- & Attack-Events

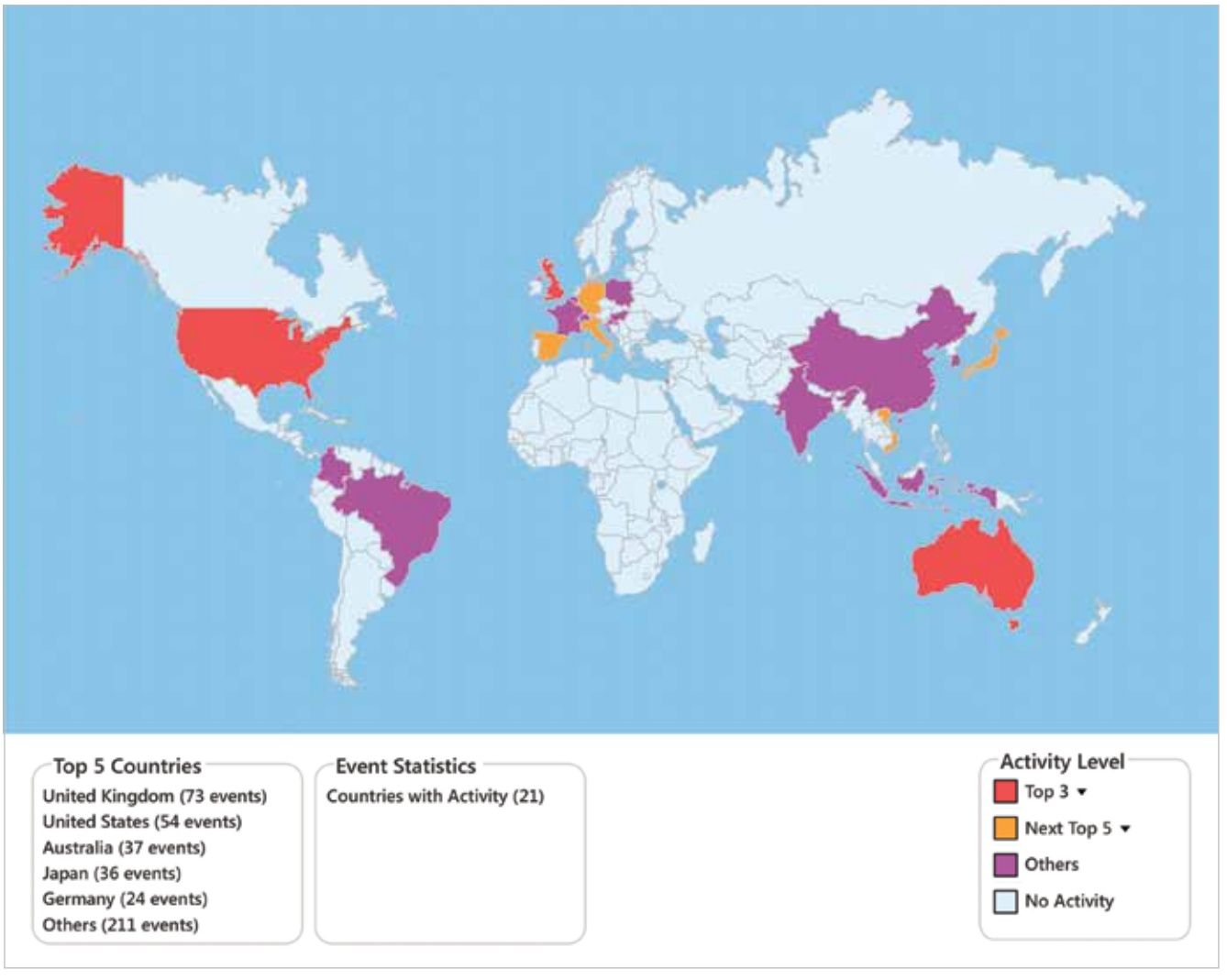
Die Check Point-Lösung identifizierte im Rahmen der Security-Analyse eine Anzahl von Vorfällen, die im Zusammenhang mit Intrusion Prevention stehen. Einige dieser Events wurden als hochgradig riskant kategorisiert. Die nachfolgende Tabelle listet die gefunden Vorfälle und den entsprechenden Schweregrad auf.

Schweregrad	Event Name	CVE-Liste*	Häufigkeit
Kritisch	Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	CVE-2012-2536	5
	Joomla Unauthorized File Upload Remote Code Execution	-	2
	Web Servers Malicious HTTP Header Directory Traversal	-	1
	ImageMagick GIF Comment Processing Off-by-one Buffer Overflow (CVE-2013-4298)	CVE-2013-4298	3
	Adobe Flash Player SWF File Buffer Overflow (APSB13-04)	CVE-2013-0633	2
Hoch	PHP php-cgi query string parameter code execution	CVE-2012-1823	1
	Oracle database server CREATE_TABLES SQL injection	CVE-2007-3890	4

*CVE (Common Vulnerabilities and Exposures) ist ein Dictionary für öffentlich bekannte Security-Schwachstellen. Weitere Informationen zu einem spezifischen IPS-Event finden Sie mithilfe der entsprechenden CVE-ID auf der National Vulnerability Database CVE-Webpage.

IPS Events nach Ländern

Nachstehende Karte zeigt die Verteilung von IPS-Events auf die jeweiligen Ursprungsländer.



03 ERGEBNISSE IM BEREICH ENDPOINT SECURITY

Dieser Abschnitt stellt die Security-Ergebnisse dar, die im Zusammenhang mit den Hosts in Ihrer Infrastruktur stehen. Er fasst diese Ergebnisse zusammen und gibt detaillierte Informationen pro Security-Vektor. Der Abschnitt „Problembehebung“ stellt Empfehlungen für die Adressierung der gefundenen Ereignisse vor.

Endpoint Security-Events – Zusammenfassung

Endpoints gesamt, auf denen hoch riskante Applikationen laufen	6
Endpoints gesamt, die in Vorfälle von Datenverlust involviert sind	19
Endpoints gesamt, die in Intrusion- & Attack-Events involviert sind	20
Endpoints gesamt, die in Malware-Vorfälle involviert sind	848

Top-Endpoints, auf denen hoch riskante Applikationen laufen

Nachfolgende Tabelle listet die Endpoint-Rechner auf, auf denen am häufigsten hoch riskante Applikationen laufen oder die auf hoch riskante Websites zugegriffen haben:

Source	Application / Site	Matched Category	App Risk
192.168.2.13	Tor	Anonymizer	5 Critical
10.10.10.235	Ultrasurf	Anonymizer	5 Critical
192.168.2.33	Coralcdn	Anonymizer	5 Critical
192.168.5.66	VTunnel	Anonymizer	5 Critical
192.168.5.33	Kugou	P2P File Sharing	5 Critical
10.10.23.235	Suresome	Anonymizer	5 Critical
172.26.35.11	Hola	Anonymizer	5 Critical
10.10.22.31	PacketiX VPN	Anonymizer	5 Critical
10.10.1.235	Kproxy	Anonymizer	5 Critical
192.168.5.39	Sopcast	P2P File Sharing	5 Critical
10.23.36.4	DarkComet-RAT	Remote Administration	5 Critical
192.168.66.3	Dropbox	File Storage and Sharing	4 High

Wichtigste Endpoints mit Intrusion- & Attack-Events

Folgende Tabelle listet die wichtigsten Endpoint-Rechner mit Intrusion Prevention-bezogenen Vorfällen auf.

Quelle	Zieladresse	Schweregrad	Event-Name	CVE-Liste
192.87.2.47	192.168.75.27	Kritisch	Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	CVE-2012-2536
192.78.2.214	192.168.75.58	Kritisch	Joomla Unauthorized File Upload Remote Code Execution	-
192.84.2.220	192.168.75.58	Kritisch	Web Servers Malicious HTTP Header Directory Traversal	-
192.85.2.133	192.168.75.58	Kritisch	ImageMagick GIF Comment Processing Off-by-one Buffer Overflow (CVE-2013-4298)	CVE-2013-4298
192.116.2.151	192.168.75.58	Kritisch	Adobe Flash Player SWF File Buffer Overflow (APSB13-04)	CVE-2013-0633
192.195.2.88	192.168.75.60	Hoch	PHP php-cgi query string parameter code execution	CVE-2012-1823
192.87.2.211	192.168.86.3	Hoch	Oracle database server CREATE_ TABLES SQL injection	CVE-2007-3890

Wichtigste Endpoints, die in Vorfälle von Datenverlust involviert sind

Nachstehende Tabelle listet die Haupt-Endpoint-Rechner auf, die von Data Loss-Events betroffen sind.

Endpoint	Events	Gesendete Daten
192.168.125.36	4	Kreditkartennummern
	1	Business-Plan
192.168.75.0	5	Finanzberichte
192.168.125.0	4	Source-Code
192.168.86.47	4	Outlook-Nachricht – Vertraulich
192.168.86.38	2	US-Sozialversicherungsnummern

Wichtigste Endpoints, die in Malware-Vorfälle involviert sind

Folgende Tabelle zeigt die Top-Endpoint-Rechner, die in Malware-bezogene Security Events involviert sind.

Host	Threat-Name	Malware-Aktivität
192.168.86.8	Operator.Virus.Win32.Sality.f.h	DNS Client Query oder DNS Server beseitigt eine C&C Site
192.168.75.0	Operator.APT1.cji	DNS Client Query oder DNS Server beseitigt eine C&C Site
192.168.75.3	Operator.Virus.Win32. Sality.d.dm	Kommunikation mit C&C
192.168.75.7	REP.yjjde	Zugriff auf bekanntlich Malware-infizierte Site
192.168.75.10	RogueSoftware.Hack_Style_ RAT.pbco	Kommunikation mit C&C
192.168.75.13	Trojan.Win32.Agent.aaeyr.cj	Download eines schadhaften Files/Exploits

COMPLIANCE SECURITY-ANALYSE

Dieser Abschnitt stellt eine detaillierte Analyse der Security Policies für Ihre bestehende Check Point Netzwerk-Security-Umgebung dar. Die Analyse wurde mithilfe des Check Point Compliance Software Blades durchgeführt, das eine umfassende Bibliothek von hunderten von Security Best Practices und Empfehlungen für eine Verbesserung der Netzwerksicherheit Ihrer Organisation nutzt.

Security Policy Compliance

Das Compliance Software Blade überprüft die Konfiguration Ihres Security-Managements, Ihrer Gateways und installierten Software Blades.

Die Ergebnisse wurden dann verglichen mit Beispielen für unsere Security Best Practices. Dabei wurde festgestellt, dass von unseren 102 empfohlenen Best Practices 67 vollständig compliant waren, jedoch 35 fehlten oder nicht mit unseren Empfehlungen konform gingen. Dies resultiert insgesamt in einem Compliance-Level von 65%.

	**65%**	Compliant mit den empfohlenen Check Point Security Best Practices
	**102**	Analysierte Security-Konfigurationen
	**67**	Configurations found compliant
	**35**	Für compliant befundene Konfigurationen
	**12**	Überwachte Security Gateways

Zusammenfassung zu den gesetzlich geregelten Compliance-Bestimmungen

Die nachstehende Tabelle stellt das Compliance-Level Ihrer Netzwerk-Security bezüglich der gesetzlich vorgegebenen Compliance-Regeln dar. Dieser Status wird durch die Analyse verschiedener Check Point Security Gateway-Konfigurationen und Software Blade-Einstellungen sowie deren Vergleich mit den gesetzlichen Anforderungen festgestellt.

Bestimmung	Anzahl der Anforderungen	Anzahl der Security Best Practices	Compliance-Status
ISO 27001	27	102	78%
PCI DSS	55	102	86%
HIPAA	16	102	78%
DSD	14	68	67%
GLBA	5	102	45%
NIST 800-41	22	25	85%
ISO 27002	198	102	77%
NIST 800-53	25	71	86%
CobiT 4.1	15	102	66%
UK Data Protection Act	1	29	49%
Firewall STIG	30	54	87%
GPG 13	9	31	87%
NERC CIP	8	56	74%
MAS TRM	25	102	77%
SOX	15	102	66%
FIPS 200	25	71	87%

Best Practices Compliance nach Security Software Blade

Nachstehende Tabelle zeigt den allgemeinen Security-Status für jedes Software Blade. Check Point empfiehlt für jedes Software Blade eine Reihe von Best Practices. Bei einem Wert von 100% wurde festgestellt, dass für dieses Blade sämtliche Best Practices richtig konfiguriert sind. Ein Wert von weniger als 100% weist auf Konfigurationen hin, die nicht mit dem empfohlenen Best Practices übereinstimmen und daher ein potentielles Sicherheitsrisiko für Ihre Umgebung darstellen.

Security Software Blade	Anzahl der Best Practices	Security-Status
Data Loss Prevention	2	7%
IPS	4	29%
Application Control	13	54%
Mobile Access	3	66%
IPSec VPN	16	73%
URL Filtering	5	87%
Firewall	35	88%
Anti-Virus	13	91%
Anti-Spam & Mail	3	100%
Anti-Bot	8	100%

Security Best Practices-Compliance: Die wichtigsten Resultate

Nachstehende Tabelle listet die wichtigsten Security Best Practices auf, die als fehlend oder nicht vollständig konfiguriert festgestellt wurden.

Blade	ID	Name	Status
Firewall	FW101	Überprüfen, ob die “Clean up”-Regel in der Firewall Rule Base definiert ist	0%
Firewall	FW102	Überprüfen, ob Anti-Spoofing auf jedem Gateway aktiviert worden ist	0%
Firewall	FW103	Überprüfen, ob Anti-Spoofing auf jedem Gateway auf Prevent eingestellt ist	0%
Firewall	FW105	Überprüfen, ob jede Firewall definierte Track Settings hat	0%
Firewall	FW130	Überprüfen, ob „Stealth Rule“ in der Firewall Rule Base definiert ist	0%
Firewall	FW152	Überprüfen, ob jede Firewall-Regel einen Namen definiert hat	0%
Firewall	FW153	Überprüfen, ob jede Firewall-Regel einen Comment definiert hat	0%
Firewall	FW107	Überprüfen, ob für jedes Gateway ein zusätzlicher Log-Server für die Speicherung der Firewall-Logs definiert ist	0%
Firewall	FW116	Überprüfen, ob NAT/PAT in den Firewall-Settings aktiviert ist	87%
Firewall	FW146	Überprüfen, ob in der Firewall Rule Base keine „Any Any Accept“-Regel definiert ist	0%
Firewall	FW159	Überprüfen, ob Feststellen, dass „Lockout Administrator\’s account after“ ausgewählt ist	0%
Firewall	FW160	Überprüfen, ob Administratoren nach 3 fehl geschlagenen Login-Versuchen ausgeloggt werden	0%
Firewall	FW161	Überprüfen, ob „Unlock Administrator\’s account after“ ausgewählt ist	0%
Firewall	FW162	Überprüfen, ob Administrator\’s accounts nach 30 Minuten entsperrt werden	0%
Firewall	FW163	Überprüfen, ob für abgemeldete Administratoren eine detaillierte Nachricht angezeigt wird	0%

05 BANDBREITEN-ANALYSE

Nachfolgender Abschnitt fasst die Bandbreitennutzung und das Webbrowsing-Profil Ihrer Organisation während der Dauer dieser Analyse zusammen.

Stärkste Bandbreitenbelegung nach Applikationen & Websites

Application / Site	Category	App Risk	Number of Users	Traffic	Number of Events
Tor	Anonymizer	5 Critical	35	149 MB	228
Ultrasurf	Anonymizer	5 Critical	33	1 GB	51
Coralcdn	Anonymizer	5 Critical	2	2 MB	45
VTunnel	Anonymizer	5 Critical	1	24 MB	18
Kugou	P2P File Sharing	5 Critical	2	7 MB	15
Suresome	Anonymizer	5 Critical	7	1 MB	9
Hola	Anonymizer	5 Critical	3	98 KB	4
PacketiX VPN	Anonymizer	5 Critical	2	300 KB	2
Kproxy	Anonymizer	5 Critical	1	400 KB	2
Sopcast	P2P File Sharing	5 Critical	1	350 KB	1
DarkComet-RAT	Remote Administration	5 Critical	1	260 KB	1
Dropbox	File Storage and Sharing	4 Critical	3573	37 GB	19,443
GoToAssist-RemoteSupport	Remote Administration	4 Critical	1573	4 GB	5,733
Lync	Instant Messaging	4 Critical	118	937 MB	1,144
TeamViewer	Remote Administration	4 Critical	182	831 MB	768
BitTorrent Protocol	P2P File Sharing	4 Critical	113	168 MB	464
Lync-sharing	Instant Messaging	4 Critical	93	70 MB	443
uTorrent	P2P File Sharing	4 Critical	2	21 MB	327
QQ IM	Instant Messaging	4 Critical	30	26 MB	294
Free Download Manager	Download Manager	4 Critical	6	373 MB	257
AOL Desktop	Anonymizer	4 Critical	47	2 MB	233
ad.adlegent.com/iframe	Spam	4 Critical	3	32 MB	228
linkuryjs.info	Spam	4 Critical	2	85 MB	227
Dropbox-web download	File Storage and Sharing	4 Critical	2	3 MB	193
LogMeIn	Remote Administration	4 Critical	39	30 MB	179
digsby	Instant Messaging	4 Critical	36	5 MB	166
ZumoDrive	File Storage and Sharing	4 Critical	17	3 MB	148
AliWangWang	File Storage and Sharing	4 Critical	2	3 MB	140

Wichtigste Web-Kategorien

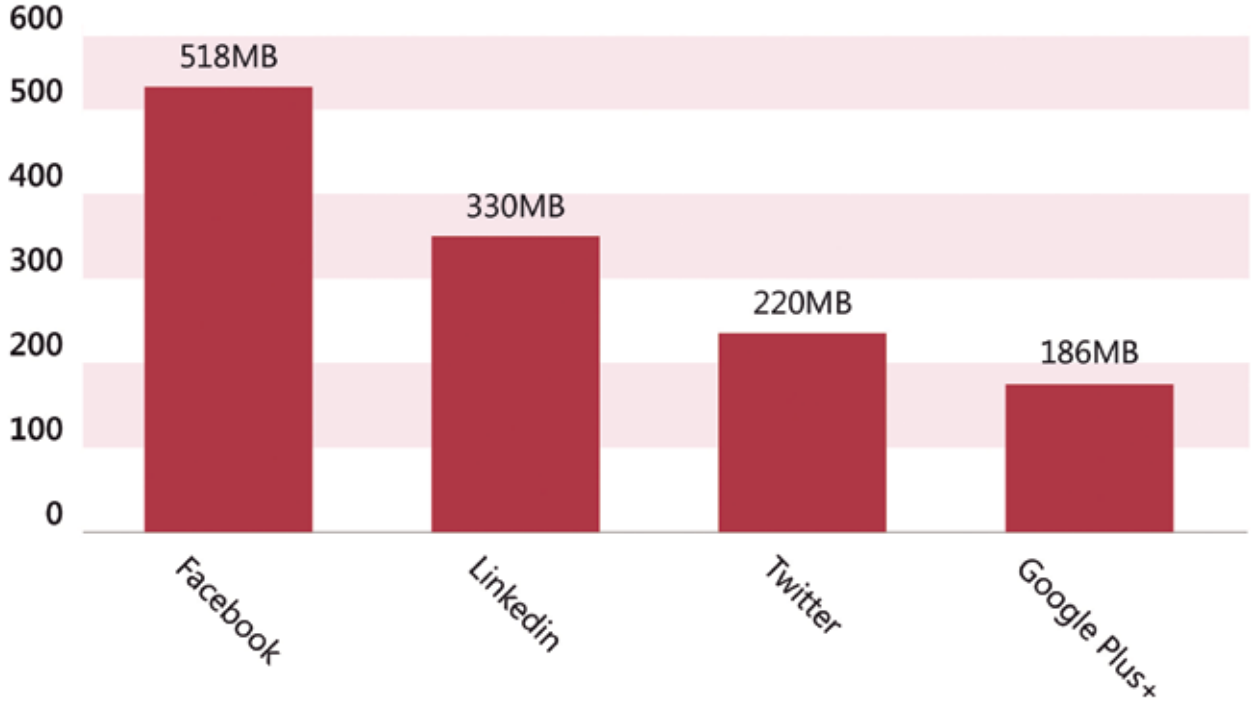
Folgende Tabelle listet die 10 meist genutzten Kategorien und die Anzahl der Treffer durch Internetnutzung der Mitarbeiter auf.

Kategorie	Anzahl Treffer	% aller Treffer
Social Networking	113	31,65%
Webmail	42	11,76%
Video Streaming	36	10,08%
Search Engines / Portals	35	9,80%
Multimedia	29	8,12%
Browser Plugin	25	7,00%
Business Applications	15	4,20%
Media Sharing	13	3,64%
Network Utilities	9	2,52%
Other	40	11,20%
Total	**357**	**100%**

Bandbreitenbelegung (MB) durch Social Networking

Die Nutzung Sozialer Netzwerke ist nicht mehr nur zu Hause sondern auch am Arbeitsplatz gebräuchlich. Viele Unternehmen nutzen Social Network-Technologien für Ihre Marketing- und Vertriebsmaßnahmen sowie ihre Personalbeschaffung.

Im Laufe dieser Analyse und in Übereinstimmung mit generell erkennbaren Markttrends belegten nachstehende Social Network-Seiten die meiste Netzwerkbandbreite:



06 EMPFEHLUNGEN FÜR DIE PROBLEMBEHEBUNG

EMPFEHLUNGEN FÜR ZUGRIFFSKONTROLLE & DATENSCHUTZ

Dieser Report adressiert in verschiedenen Security-Bereichen identifizierte und unterschiedlich kritische Sicherheitsvorfälle.

Nachstehende Tabelle fasst die kritischsten dieser Vorfälle zusammen und stellt Ansätze vor, die damit verbundenen Risiken zu entschärfen.

Check Point bietet zahlreiche Methoden für die Adressierung dieser Gefahren und entsprechender Sicherheitsbedenken an. Für jeden Sicherheitsvorfall werden anhand des Software Blades, das die hierfür geeigneten Abwehrmechanismen umfasst, die entsprechend relevanten Schutzmaßnahmen vorgestellt.

Empfehlungen für die Problembehebung bei Web Security-Events

Applikation/Site	App.-Risiko	Vorfälle	Schritte zur Abhilfe
Tor	Kritisch	228	Mit Hilfe der Application Control- und URL Filtering-Software Blades können Sie die Nutzung aller genannten Applikationen und Websites aktivieren, nachverfolgen und unterbinden. Sie können eine granulare Policy definieren, um z. B. nur bestimmten Gruppen die Nutzung bestimmter Applikationen zu erlauben. Nutzen Sie UserCheck um • die Anwender über die Regeln für die Web- und Applikationsnutzung im Unternehmen aufzuklären • Ihre Anwender sofort darüber zu informieren, wenn deren Aktionen die Security Policy verletzen.
Ultrasurf	Kritisch	51	
Vtunnel	Kritisch	18	
BitTorrent	Hoch	464	
ZumoDrive	Hoch	148	

Weitere Informationen hierzu finden Sie unter **http://www.checkpoint.com/products/application-control-software-blade/index.html** und **http://www.checkpoint.com/products/url-filtering-software-blade/.**

Empfehlungen für die Problembehebung bei Data Loss-Events

<table>
<tr><th>Schweregrad</th><th>Daten</th><th>Events</th><th>Schritte zur Abhilfe</th></tr>
<tr><td>Kritisch</td><td>Kreditkartennummern</td><td>14</td><td rowspan="6">Aktivieren Sie das DLP Software Blade, um die entdeckten Vorfälle zu beheben. Konfigurieren Sie eine DLP Policy, basierend auf dem entdeckten DLP-Datentyp, und wählen Sie eine Aktion (Erkennen/Verhindern/Benutzer fragen/etc.). Wenn Sie den entdeckten Datentyp als sensitive Information einstufen, ist die empfohlene Aktion „Verhindern”.

Setzen Sie UserCheck ein, um
• die Mitarbeiter über die Datennutzungsregeln im Unternehmen aufzuklären.
• den Mitarbeitern sofortige Rückmeldung zu geben, wenn ihre Aktivitäten die Sicherheitsregeln für die Datennutzung verletzen.</td></tr>
<tr><td rowspan="4">Hoch</td><td>Business-Plan</td><td>1</td></tr>
<tr><td>Finanzberichte</td><td>3</td></tr>
<tr><td>Source Code</td><td>12</td></tr>
<tr><td>Outlook-Nachricht, vertraulich</td><td>147</td></tr>
<tr><td rowspan="2">Mittel</td><td>Lohnabrechnung</td><td>25</td></tr>
<tr><td>US-Sozialversicherungsnummern</td><td>15</td></tr>
</table>

Für weitere Informationen klicken Sie auf
http://www.checkpoint.com/products/dlp-software-blade/index.html

EMPFEHLUNGEN FÜR THREAT PREVENTION

Empfehlungen für die Problembehebung bei Vorfällen von Malware

Malware	Schweregrad	Events	Schritte zur Abhilfe
REP.yjjde	Kritisch	36	Aktivieren Sie das Check Point Anti-Bot Software Blade, um Bot-infizierte Rechner zu erkennen und entsprechende Schäden zu verhindern. Aktivieren Sie das Check Point Anti-Virus Software Blade, um das Herunterladen von Malware zu verhindern. Aktivieren Sie das Check Point Threat Emulation Software Blade für den Schutz vor neuen und unentdeckten Malware-Gefahren. Für die Wiederherstellung einer infizierten Maschine finden Sie im Check Point ThreatWiki weitere Informationen zu der gefundenen Malware und Empfehlungen zur Fehlerbeseitigung. Folgen Sie im nächsten Schritt den Problembehebungsinstruktionen auf der „Malware Remediation Steps“-Webpage.
Operator.Virus.Win32.Sality.d.dm	Kritisch	28	
Operator.Conficker.bhvl	Hoch	27	
Operator.Zeus.bt	Hoch	11	
Operator.BelittledCardigan.u	Hoch	8	

Weitere Informationen hierzu finden Sie auf

http://www.checkpoint.com/products/anti-bot-software-blade/index.html

http://www.checkpoint.com/products/antivirus-software-blade/

http://www.checkpoint.com/products/threat-emulation/.

Empfehlungen für die Problembehebung bei Intrusion- & Attack-Events

Gefährdung	Schweregrad	Events	Schritte zur Abhilfe
Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	Kritisch	15	Aktivieren Sie folgende Schutzvorrichtung im Check Point IPS Software Blade: **Microsoft SCCM Reflected Cross-site Scripting (MS12-062)**
Joomla Unauthorized File Upload Remote Code Execution	Kritisch	13	Aktivieren Sie folgende Schutzvorrichtung im Check Point IPS Software Blade: **Joomla Unauthorized File Upload Remote Code Execution**
Microsoft Active Directory LSASS Recursive Stack Overflow [MS09-066]	Hoch	4	Aktivieren Sie folgende Schutzvorrichtung im Check Point IPS Software Blade: **Microsoft Active Directory LSASS Recursive Stack Overflow [MS09-066]**

Weitere Informationen hierzu finden Sie unter **http://www.checkpoint.com/products/ips-software-blade/**.

EMPFEHLUNGEN FÜR DIE PROBLEMBEHEBUNG BEI ENDPOINT SECURITY-EVENTS

Dieser Abschnitt adressiert identifizierte Endpoint Security-Events in verschiedenen Security-Bereichen und von unterschiedlichem Schweregrad. Die nachstehenden Tabellen zeigen die kritischsten dieser Vorfälle auf und stellen Ansätze vor, die damit verbundenen Risiken zu entschärfen.

Check Point bietet zahlreiche Methoden für die Adressierung dieser Gefahren und entsprechenden Sicherheitsbedenken an. Für jeden Sicherheitsvorfall werden anhand der Endpoint Software Blades, die die hierfür geeigneten Abwehrmechanismen umfassen, die entsprechend relevanten Schutzmaßnahmen vorgestellt.

Web Security Events – Empfehlungen für die Problembehebung am Endpoint

Host	Applikation/Site	Risiko	Schritte zur Abhilfe
192.168.75.36	Tor	Kritisch	**Check Point Endpoint Security** kontrolliert die Nutzung hoch riskanter Applikationen und Websites selbst dann, wenn sich der Endpoint außerhalb des Unternehmensnetzwerks befindet und keine Netzwerk-Security-Lösung aufweist. Nutzen Sie das **Check Point Program Control Software Blade** um nur genehmigte Programme auf dem Endpoint zuzulassen und nicht genehmigte oder nicht vertrauenswürdige Programme zu unterbinden. Nutzen Sie das **WebCheck Endpoint Software Blade** um das Unternehmen vor Web-basierten Gefahren wie Driveby-Downloads, Phishing Sites und Zero-day-Attacken zu schützen. Nutzen Sie das **Check Point Compliance Check Software Blade** um festzustellen, ob ein bestimmtes Programm auf dem Endpoint-Gerät ausgeführt wird und begrenzen Sie dessen Netzwerkzugriff, soweit erforderlich. Kontrollieren Sie den eingehenden und ausgehenden Datenverkehr mit dem **Endpoint Firewall Software Blade** um den Zugriff auf spezifische Ports und Netzwerk-Services einzuschränken. Nutzen Sie **UserCheck** um: • Die Mitarbeiter über die Nutzungsregeln Ihres Unternehmens für Browser und Applikationen aufzuklären • Die Nutzer sofort zu informieren, wenn ihre Aktivitäten gegen die Security Policy verstoßen.
192.168.75.71	Ultrasurf	Kritisch	
192.168.86.0	VTunnel	Kritisch	
192.168.86.19	BitTorrent	Hoch	
192.168.86.30	ZumoDrive	Hoch	

Hier erhalten weitere Informationen zu den Check Point Endpoint Security Software Blades:

• Zum Program Control Endpoint Security Software Blade unter:
http://www.checkpoint.com/products/anti-malware-program-control/index.html

• Zum WebCheck Endpoint Security Software Blade unter:
http://www.checkpoint.com/products/webcheck/index.html

• Zum Compliance Check Endpoint Security Software Blade unter:
http://www.checkpoint.com/products/firewall-compliance-check/index.html

• Zum Firewall Endpoint Security Software Blade unter:
http://www.checkpoint.com/products/firewall-compliance-check/index.html

Intrusion & Attack Events – Empfehlungen für die Problembehebung am Endpoint

Quelle	Zieladresse	Event-Name	Schritte zur Abhilfe
192.87.2.47	192.168.75.27	Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	Nutzen Sie das **Endpoint Compliance Software Blade** um zu prüfen, ob die Endpoints in Ihrer Organisation mit den jüngsten Security-Patches und Updates aktualisiert sind. Das **Endpoint Compliance Software Blade** wird sicherstellen, dass die Endpoints selbst dann geschützt sind, wenn sie sich außerhalb des Unternehmensnetzwerks befinden und keinen Netzwerk-Security-Schutz haben, etwa beim Arbeiten von zu Hause oder von unterwegs aus.
192.78.2.214	192.168.75.58	Joomla Unauthorized File Upload Remote Code Execution	
192.84.2.220	192.168.75.58	Web Servers Malicious HTTP Header Directory Traversal	
192.85.2.133	192.168.75.58	ImageMagick GIF Comment Processing Off-by-one Buffer Overflow (CVE-2013-4298)	
192.116.2.151	192.168.75.58	Adobe Flash Player SWF File Buffer Overflow (APSB13-04)	
192.195.2.88	192.168.75.60	PHP php-cgi query string parameter code execution	
192.87.2.211	192.168.86.3	Oracle database server CREATE_TABLES SQL injection	

Sie erhalten weitere Informationen zu nachstehenden Check Point Endpoint Security Software Blades unter:

- Firewall Endpoint Security Software Blade – **http://www.checkpoint.com/products/firewall-compliance-check/index.html** und
- Compliance Check Endpoint Security Software Blade – **http://www.checkpoint.com/products/firewall-compliance-check/index.html**

Data Loss Events – Empfehlungen für die Problembehebung am Endpoint

Host	Typ	Schritte zur Abhilfe
192.168.75.0	Kreditkartennummern	Nutzen Sie das **Check Point Full Disk Encryption Software Blade** um sensitive Informationen auf Endpoint-Festplatten einschließlich Benutzerdaten, Betriebssystemdateien und temporäre oder gelöschte Dateien vor unerlaubtem Zugriff zu schützen, wenn Laptops verloren gehen oder gestohlen werden. Nutzen Sie das **Check Point Media Encryption Software Blade** für die Verschlüsselung sensitiver Daten, die auf mobilen Datenträgern hinterlegt sind, sowie für die individuelle Verwaltung dieser Devices. Durch den Einsatz des **Check Point Document Security Software Blades** gestatten Sie den Zugriff auf sensitive Dokumente ausschließlich den dafür autorisierten Personen. Setzen Sie **UserCheck ein**, um • die Mitarbeiter über die Datennutzungsregeln im Unternehmen aufzuklären. • den Mitarbeitern sofortige Rückmeldung zu geben, wenn ihre Aktivitäten die Sicherheitsregeln für die Datennutzung verletzen.
192.168.86.47	Business-Plan	
192.168.125.0	Source-Code	
192.168.125.36	Lohnabrechnung	

Klicken Sie auf nachstehende Links, um weitere Informationen zu folgenden **Check Point Endpoint Software Security Blades** zu erhalten:

- Full Disk Encryption Endpoint Security Software Blade:
  http://www.checkpoint.com/products/full-disk-encryption/index.html
- Media Encryption Endpoint Security Software Blade:
  http://www.checkpoint.com/products/media-encryption/index.html
- Document Security Endpoint Security Software Blade:
  https://documentsecurity.checkpoint.com/ds-portal/

Malware Events – Empfehlungen für die Problembehebung am Endpoint

Host	Schweregrad	Schritte zur Abhilfe
192.53.2.161	Kritisch	Nutzen Sie das **Check Point Endpoint Anti-Malware Software Blade** um Gefahren wie Malware, Viren, Keystroke Logger, Trojaner und Root Kits zu erkennen und Ihre Endpoints vor Infektionen zu schützen. Das **Check Point Endpoint Anti-Malware Software Blade** wird Ihre unternehmensweiten Endpoints auch dann schützen, wenn sie sich außerhalb des Unternehmensnetzwerks befinden und nicht über einen Netzwerk-Security-Schutz verfügen, etwa beim Arbeiten von zu Hause oder von unterwegs aus. Setzen Sie das **Endpoint Compliance Software Blade** ein um sicherzustellen, dass die Endpoints mit den jüngsten Security-Updates aktualisiert sind und mit der Security-Policy Ihrer Organisation konform gehen. Zur Unterstützung der Problembehebung auf einem infizierten Rechner finden Sie im **Check Point ThreatWiki** zusätzliche Informationen und Lösungsempfehlungen zur gefundenen Malware und den damit verbundenen, potentiellen Risiken. Nutzen Sie **UserCheck** um Ihre Mitarbeiter über die Nutzungsregeln für den Einsatz von Webbrowsern und Applikationen in Ihrem Unternehmen aufzuklären.
192.57.2.32	Kritisch	
192.57.2.209	Kritisch	
192.59.2.27	Kritisch	
192.59.2.79	Kritisch	

Klicken Sie auf nachstehende Links, um weitere Informationen zu folgenden Check Point Endpoint Software Security Blades zu erhalten:

- Anti-Malware Endpoint Security Software Blade:
  http://www.checkpoint.com/products/anti-malware-program-control/index.html
- Firewall & Compliance Check Endpoint Security Software Blade:
  http://www.checkpoint.com/products/firewall-compliance-check/index.html

Durchführung eines umfassenden Endpoint Security Analysis-Reports

Für eine umfassendere Analyse Ihrer Endpoints im Hinblick auf deren Security-Status und potentielle Risiken führen Sie den Endpoint Security Analysis-Report aus oder kontaktieren Sie den lokal für Sie zuständigen Check Point-Repräsentanten.

COMPLIANCE BLADE – EMPFEHLUNGEN FÜR DIE PROBLEMBEHEBUNG

Dieser Report adressiert identifizierte Security-Konfigurationen, die sich über sämtliche Check Point Software Blades hinweg auswirken und zu beachten sind.

Nachstehende Tabelle listet einige dieser Konfigurationen auf und gibt Anleitung für eine Verbesserung des Security-Levels.

Risiko	Schritte zur Abhilfe	Relevante Objekte
Hoch	Erstellen Sie eine neue Stealth Rule oder modifizieren die bestehende Stealth Rule in den relevanten Policy Packages in Übereinstimmung mit der folgenden Definition: Source = Any ; Destination = GW's ; Service = Any ; Action = Drop ; Install On = Policy Target ; Time = Any.	Policy Package A
Hoch	Erstellen Sie eine neue Clean-up-Rule oder modifizieren Sie die bestehende Clean-up-Rule in den relevanten Policy Packages in Übereinstimmung mit der folgenden Definition: Source = Any ; Destination = Any; VPN = Any Traffic ; Service = Any ; Action = Drop; Track = Log; Install On = Policy Targets; Time = Any; Beachten Sie, dass die Clean-up-Rule die letzte in der Firewall Rule Base aufgeführte Zeile sein muss.	Policy Package B
Hoch	Aktivieren Sie das automatische Updaten der Schutzvorrichtungen im IPS Blade	IPS Gateway Corporate Gateway
Hoch	Erstellen Sie eine neue Policy oder modifizieren Sie die bestehende Policy im Application Control Blade, so dass kritische Risiko-Applikationen und Websites blockiert werden	Policy Package A
Hoch	Modifizieren Sie die Timeout-Settings für die Authentifizierung in den Global Properties, so dass sie zwischen 20 und 120 Minuten liegen. Global Properties	Global Properties
Hoch	Definieren Sie ein Track-Setting für sämtliche Firewall-Regeln über alle Policy Packages hinweg.	Policy Package A — Regelnummer 18 — Regelnummer 35 — Regelnummer 64 Policy Package B — Regelnummer 11 — Regelnummer 23 — Regelnummer 88

SOFTWARE-DEFINED PROTECTION

Heutige IT-Infrastrukturen und Netzwerke sind nicht nur erheblich komplexer und anspruchsvoller, als noch vor einigen Jahren. Sie sind einem steten Wandel unterworfen und weisen vor allem auch keine klar definierten Grenzen mehr auf. Damit stehen sie nicht nur für den erwünschten Zugriff durch mobile Mitarbeiter und Drittanbieter offen, sondern auch für immer neue, immer intelligentere Sicherheitsgefahren. Wie können sich Unternehmen dennoch nachhaltig schützen?

Meist setzen die Organisationen bereits zahlreiche, punktuelle Security-Produkte ein – Produkte, die von ihrem Ursprung her aber eher reaktiv und taktisch als architektonisch ausgerichtet sind. Moderne Unternehmen benötigen dagegen eine einzige Architektur, die hoch performante Vorrichtungen für die Netzwerk-Security mit proaktiven, in Echtzeit arbeitenden Schutzmaßnahmen verbindet.

Wollen wir heutige Organisationen proaktiv schützen, müssen wir also umdenken, ein neues Paradigma entwerfen.

Software-Defined Protection (SDP) ist eine neue, pragmatische Security-Architektur und Methodologie. Sie bietet eine Infrastruktur, die modular, agil und vor allem SICHER ist.

Eine solche Architektur muss in der Lage sein, Unternehmen ganz unabhängig von ihrer Größe und ihrem Standort zu schützen, sowohl die Netzwerke in der Zentrale als auch die in den Zweigstellen, das Roaming über Smartphones und andere mobile Endgeräte und auch die Nutzung von Cloud-Umgebungen.

Die Schutzmaßnahmen sollten sich automatisch an veränderte Gefährdungen anpassen, so dass sich Security-Administratoren nicht manuell mit zahllosen Ratschlägen und Empfehlungen beschäftigen müssen. Sie müssen sich außerdem nahtlos in die übergreifende IT-Umgebung einbinden lassen, und die Architektur muss eine schützende Basis bilden, die sowohl die bereits vorhandenen internen als auch externen Ressourcen intelligent und kollaborativ zu nutzen weiß.

Die Software-Defined Protection-Architektur unterteilt die Security-Infrastruktur in drei miteinander verbundene Ebenen:

- Einen **Enforcement Layer, der** auf physischen, virtuellen und Host-basierten Lösungen für die Durchsetzung der Security beruht und sowohl das Netzwerk segmentiert, als auch die hinter den Schutzmaßnahmen stehende Logik selbst in sehr anspruchsvollen Umgebungen ausführt.
- Einen **Control Layer**, der unterschiedliche Quellen zu Gefährdungsinformationen analysiert und Schutzmaßnahmen sowie Policies generiert, die von dem Enforcement Layer ausgeführt werden.
- Einen **Management Layer**, der die gesamte Infrastruktur orchestriert und für die gesamte Architektur ein Höchstmaß an Agilität sicherstellt.

Die Software-Defined Protection (SDP)-Architektur

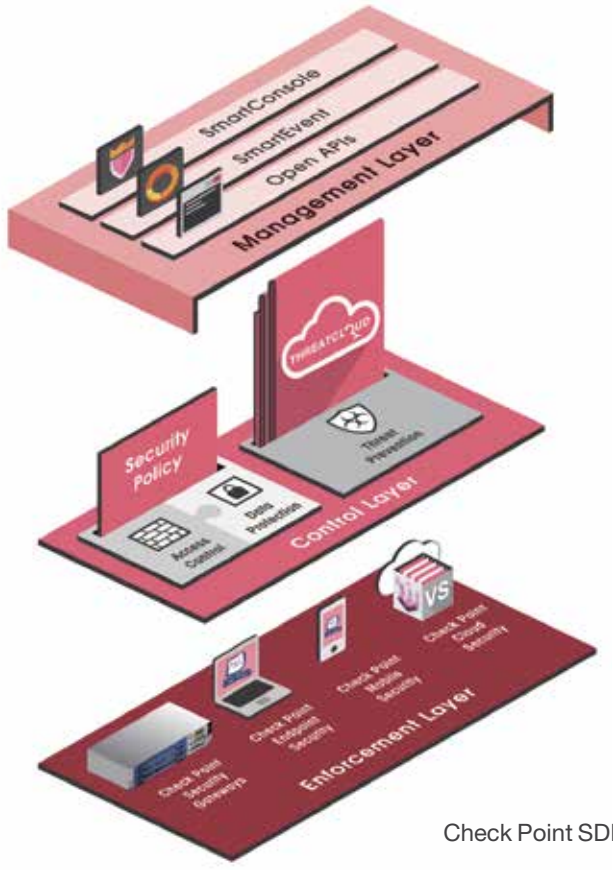
Durch die Kombination des hoch performanten Enforcement Layers mit dem sich kontinuierlich entwickelnden, dynamischen und Software-basierten Control Layer bietet die SDP-Architektur nicht nur eine hohe, operative Belastbarkeit, sondern sorgt auch für die proaktive Abwehr sich stetig ändernder Gefahren.

Auf die Zukunft ausgelegt, unterstützt die SDP-Architektur sowohl traditionelle Anforderungen an Policies für die Netzwerk-Security und Zugriffskontrolle, als auch neue Herausforderungen an die Gefahrenprävention, wie sie für heutige Unternehmen erforderlich ist, die auf moderne Technologien wie Mobile Computing und Software-definierte Netzwerke (SDN) setzen.

CHECK POINT SOFTWARE-DEFINED PROTECTION

Check Point stellt sämtliche Komponenten zur Verfügung, die für die Implementierung einer vollständigen SDP-Architektur mit herausragendem Management und bestmöglicher Security erforderlich sind.

Die Software-definierten Schutzvorrichtungen von Check Point halten jederzeit flexibel mit neuen Gefahren Schritt und beziehen neue Technologien ein. Unsere Lösungen generieren neue und aktualisierte Schutzmaßnahmen für bekannte und unbekannte Gefährdungen und stellen das neu gewonnene Wissen proaktiv in die Cloud. Die Implementierung der Check Point Security-Lösungen auf Basis dieses fundierten, architektonischen Security-Designs gibt Unternehmen die Möglichkeit, selbst modernste Informationssystemlösungen bedenkenlos in ihre Umgebungen zu integrieren.



Check Point SDP

CHECK POINT SDP-ENFORCEMENT LAYER

Für die Absicherung der Grenzen jedes Netzwerksegments bietet Check Point eine Vielzahl von Lösungen, sog. Enforcement Points, die für die Durchsetzung der Security sorgen. Dazu gehören hoch performante Netzwerk-Security-Appliances, virtuelle Gateways, Endpoint-Host-Software und Applikationen für mobile Endgeräte. Check Point gibt Unternehmen sämtliche Komponenten an die Hand, die für den Aufbau segmentierter, konsolidierter und sicherer Systeme und Netzwerke erforderlich sind.

CHECK POINT SDP-CONTROL LAYER

Der Check Point SDP Control Layer beruht auf der Check Point Software Blade-Architektur, auf deren Basis der Kunde flexible und effektive Security-Lösungen erhält, die exakt seinen Erfordernissen entsprechen. Bei einer Auswahl von mehr als 20 Software Blades ermöglicht die modulare Natur der Software Blade-Architektur dem Kunden zunächst eine relevante Security-Lösung für einen bestimmten Enforcement Point zu erstellen und – bei Bedarf – seine Security Infrastruktur später allmählich auszubauen.

Next Generation Threat Prevention

Check Point stellt effiziente, automatisierte Kontrollen zur Verfügung, die vielen der bekannten und unbekannten Gefährdungen entgegen wirken. Die Check Point Threat Prevention-Lösung umfasst: ein integriertes Intrusion Prevention System (IPS), Netzwerk-basiertes Anti-Virus, Threat Emulation und Anti-Bot.

Darüber hinaus hat Check Point mit Check Point ThreatCloud™ eine einzigartige, Cloud-basierte Lösung entwickelt, die aus großen Datenmengen intelligente Informationen zu Gefährdungen und Schutzmaßnahmen generiert.

Check Point ThreatCloud unterstützt die kollaborative Bekämpfung des Cybercrime, indem die Lösung dem Control Layer in Echtzeit intelligente, zu Security-Indikatoren konvertierte Threat-Informationen zur Verfügung stellt.

Next Generation Firewall und Data Protection

Die Check Point-Zugriffskontrolle basiert auf unserer Next Generation Firewall in Kombination mit zahlreichen Software Blades und ermöglicht damit eine einheitliche, Kontext-basierte Security Policy: Next Generation Firewall und VPN, User Identity Awareness, Application Control, Daten- und Content Awareness.

Next Generation Data Protection

Check Point Next Generation Data Protection erweitert die Lösung um Data Awareness. Sie umfasst unser Data Loss Prevention (DLP) Software Blade, das die Überprüfung von Content ausführt und die Inhalte von Files mit Dateien abgleicht, die in den Repositories des Unternehmens hinterlegt sind. Darüber hinaus bietet Check Point Verschlüsselungstechnologien für den Schutz von Daten im Ruhezustand sowie abgespeicherten Daten an. Diese Technologien können an allen Enforcement Points implementiert werden. Sie schützen sensitive Dokumente und vertrauliche Daten vor dem Zugriff oder der Übertragung auf mobile Datenträger durch nicht autorisierte Nutzer.

CHECK POINT SDP-MANAGEMENT LAYER

Sämtliche Schutzvorrichtungen und Enforcement Points von Check Point werden über eine einzige, einheitliche Security Management-Konsole verwaltet. Das hoch skalierbare Check Point Security Management ist in der Lage, Millionen von Objekten zu verwalten und bietet gleichzeitig extrem schnelle Antwortzeiten.

Modulares/mehrschichtiges Check Point Policy Management

Check Point Security Management unterstützt die unternehmensweite Segmentierung, so dass Administratoren für jedes Segment eine spezifische Security Policy definieren und dabei anhand des neuen „Layers und Sub Layers"-Konzepts eine Aufgabentrennung durchsetzen können. Policies können für jedes Segment definiert werden. Policies für die Zugriffskontrolle können unter Nutzung verschiedener Layer definiert werden, die verschiedenen Administratoren zugeordnet werden können. So können dann mehrere Administratoren simultan an der gleichen Policy arbeiten.

Automation und Steuerung

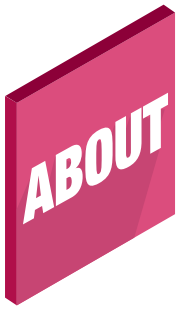
Check Point Security Management bietet CLIs und Webservice-APIs, die Unternehmen die Integration mit anderen Systemen wie Netzwerkmanagement, CRM, Trouble-Ticketing, Identity Management und Cloud-Steuerung erlauben.

Überblick mit Check Point SmartEvent

Check Point SmartEvent führt Big Data-Analysen und die Echtzeit-Korrelation von Security-Vorfällen aus. Es bietet die Möglichkeit, auf Basis mehrerer Informationsquellen eine konsolidierte und korrelierte Übersicht zu einem spezifischen Vorfall zu erstellen. Die Analyse der Security-Events liefert anwendbare, intelligente Informationen in Form von Threat-Indikatoren, die über die ThreatCloud verbreitet und so die erkannten Gefährdungen in Echtzeit blockieren können.

Event Management mit Check Point SmartEvent

Erfahren Sie mehr über Check Point Software Defined Protection (SDP) und wie Sie diese innovative Architektur dabei unterstützen kann, dass Ihre Security-Infrastruktur mit immer neuen, sich stetig ändernden Gefahren für Ihre Geschäftsdaten Schritt halten kann. Besuchen Sie uns unter **www.checkpoint.com/securitycheckup**.



ÜBER CHECK POINT SOFTWARE TECHNOLOGIES

Check Point Software Technologies **http://www.checkpoint.com/** gehört zu den führenden Anbietern von Lösungen für die Absicherung des Internets. Das Unternehmen wurde 1993 gegründet und hat seither Technologien entwickelt, um die Kommunikation und Transaktionen von Unternehmen und Verbrauchern im Internet zu schützen.

Mit FireWall-1 und seiner patentierten Stateful Inspection-Technologie war Check Point Pionier am Markt für Security-Technologie. Durch die Entwicklung unserer Software Blade-Architektur haben wir unsere IT Security-Innovationen jetzt weiter ausgebaut. Die dynamische Software Blade-Architektur bietet sichere, flexible und einfach zu nutzende Lösungen, die an die spezifischen Security-Anforderungen jedes Unternehmens und jeder Umgebung angepasst werden können.

Check Point entwickelt und vermarktet eine breite Palette von Software sowie Produktkombinationen aus Software-, Hardware- und Servicelösungen für die IT Security. Wir bieten unseren Kunden ein umfassendes Portfolio von Netzwerk- und Gateway Security-Lösungen an, sowie Daten-, Endpoint Security- und Management-Lösungen. Unsere Produkte arbeiten unter dem Dach einer einheitlichen Security-Architektur, die mit nur einer Produktreihe aus einheitlichen Security Gateways durchgängige End-to-End-Security ermöglicht. Dabei wird die gesamte Endpoint-Security mithilfe eines einzigen Agenten über nur eine, einheitliche Managementkonsole verwaltet. Dieses einheitliche Management ermöglicht den einfachen Einsatz der Produkte sowie deren zentrale Kontrolle und wird durch Echtzeit-Security-Updates unterstützt und aktualisiert.

Unsere Produkte und Services werden für Organisationen, Service Provider, kleine und mittelgroße Unternehmen und Endverbraucher angeboten. Unsere „Open Platform for Security“ (OPSEC)-Struktur ermöglicht Anwendern den Ausbau unserer Produkt- und Service-Kapazitäten mit Hardware- und Security Software-Anwendungen von Drittanbietern. Unsere Produkte werden über unser weltweites Partnernetzwerk vertrieben, integriert und gepflegt. Zu unseren Kunden gehören Zehntausende von Organisationen und Unternehmen aller Größen, einschließlich aller Fortune 100-Unternehmen. Unsere mehrfach mit Preisen ausgezeichneten ZoneAlarm-Lösungen schützen Millionen von Verbrauchern vor Hackern, Spyware und Identitätsdiebstahl.