DATIS®

Unified Threat Management by DATIS

Wie Sie Ihre IT-Sicherheit auf die sichere Seite bringen.

Laut Bitkom war 2018 jeder zweite Internetnutzer (50 Prozent) im vergangenen Jahr Opfer von Cyberkriminalität. Am häufigsten klagen Onliner über die illegale Verwendung ihrer persönlichen Daten oder die Weitergabe ihrer Daten an Dritte. Fast jeder Vierte (23 Prozent) war davon betroffen. Das ist das Ergebnis einer repräsentativen Umfrage im Auftrag des Digitalverbands Bitkom unter mehr als 1.000 Internetnutzern in Deutschland. So wurden im vergangenen Jahr 12 Prozent der Internetnutzer nach eigenen Angaben beim privaten Einkauf oder Verkaufsgeschäften betrogen. Jeder Neunte (11 Prozent) gibt an, dass seine Kontodaten missbraucht wurden. Nur 2 Prozent berichten jeweils von Datenklau und Identitätsdiebstahl außerhalb des Internets, den Missbrauch von Kontodaten gibt dort 1 Prozent an.

Kaum ein anderer Bereich der Unternehmens-IT steht permanent weltweit so unter Dauerfeuer wie die IT-Security. Dabei spielt die Größe des Unternehmens für die Bewertung der Bedrohungsszenarien durch Viren, Trojaner, Malware oder Hackerangriffe kaum eine Rolle. Betroffen davon sind mittelständische Unternehmen genauso wie Konzerne.

Unabhängig von der DSGVO steigen die Anforderungen an die IT-Sicherheit ständig. Ein Malwarebefall oder ein Hackerangriff kann je nach Ausprägung neben dem Imageschaden zu erheblichen Betriebsstörungen bis hin zu Datenverlust und Datendiebstahl verbunden mit enormen wirtschaftlichen Verlusten führen. Daher gilt es, im ständigen Wettrüsten nicht den Anschluss zu verlieren.

Als Full Service Hosting Provider beobachten wir den Security Markt ständig, um unseren Kunden, ihren Mitarbeiter/Innen, Geschäftspartnern und Endkunden die besten Sicherheitslösungen anbieten zu können, die Ihrem individuellen Bedarf entsprechen.

Dabei setzen wir auf ein Bündel von Maßnahmen, die durch moderne Hardware- und Software-Technologien unterstützt wird:

Web Protection

Wireless Protection

Network Protection

Sandstorm Sandboxing

E-Mail Protection

Webserver Protection

Für den Gateway-Betrieb in Richtung Internet setzen wir eine sogenannte Unified Threat Management (UTM) Firewall des Herstellers Sophos ein. Diese UTM bietet verschiedene Technologien einerseits zum Schutz und andererseits zur Kontrolle und Filterung des Datenverkehrs zwischen dem Internet und dem Unternehmens-Netzwerk.

Ein solcher Service ist für jedes Unternehmen notwendig, um den aktuellen Anforderungen an die IT-Security gerecht zu werden.

DATIS®

DATIS kann seinen Kunden diesen Service in drei Stufen anbieten:

BASIS

Der minimale Basis-Schutz ist grundsätzlicher Bestandteil jedes Servicevertrags.

SHARED

Die Lizenzierung erfolgt pro User/IP-Adresse.
Beispiel: 5 Server im Rechenzentrum; 25 Mitarbeiter mit PC; Davon 5 Mitarbeiter mit zusätzlichem Notebook —> Lizenziert werden 5+25+5=35

DEDIZIERT

Die Lizenzierung erfolgt pro User/IP-Adresse wie in der Lizenzierungsart SHARED - mit der Ausnahme, dass es nur Lizenzpakete in den Stufen 10, 25, 50, 75, 100, 150, 250, 500, 750, 1000, 1500, 2500, Unlimited gibt. Optionale Features müssen zusätzlich lizenziert werden.

Feature	BASIS	SHARED	DEDIZIERT
Firewall (Paketfilter)	X	X	X
HTTP Malware Scanning		X	X
HTTPs Malware Scanning		INDIVIDUELL	INDIVIDUELL
URL-Filter		DEFAULT	INDIVIDUELL
FTP Malware Scanning (FTP-Proxy)		INDIVIDUELL	INDIVIDUELL
Application Control			X
E-Mail Malware Scanning		X	X
E-Mail Antispam / Quarantäne-Report		X	INDIVIDUELL
E-Mail Attachment-Filter		DEFAULT	INDIVIDUELL
E-Mail Real Time Blacklist		DEFAULT	INDIVIDUELL
E-Mail Blacklist / Whitelist für Absender/Empfänger			INDIVIDUELL
Mail-Empfang/-Versand über externen Provider (z.B. Strato,1&1, etc.)	DEFAULT	EINGESCHRÄNKT	X
Mail-Empfang/-Versand direkt über MX-Record		SHARED IP	EIGENE IP
Mailverschlüsselung (s/Mime und PGP)	CLIENT	CLIENT	X
Sandstorm Technology			(optional)
Intrusion Prevention System		X	X
Advanced Threat Protection		X	X
Web Server Protection (Application Firewall)			X
Self-Service-Portal für Benutzer			X
Protokollierung & Reporting			X

DATIS®

Firewall (Paketfilter)

Die Firewall ist der Torwächter zwischen Ihren internen Netzen und dem öffentlichen Internet. Nur zugelassene Dienste dürfen die Firewall passieren.

HTTP Malware Scanning

Schutz vor Malware beim Internet-Surfen auf unverschlüsselten Webseiten.
Zusätzliche können Dateien mit bestimmten Dateiendungen vom Herunterladen ausgeschlossen werden.
Per Default sind folgende Dateiendungen beim Herunterladen nicht erlaubt:
com, bat, vbx, hta, inf, jse, wsh, vbs, vbe, lnk, chm, pif, reg, scr, cmd, exe, msi

HTTPS Malware Scanning

Schutz vor Malware beim Internet-Surfen auf verschlüsselten Webseiten.
Immer mehr Webseiten bieten ihre Dienste nur noch verschlüsselt per HTTPs an. Einerseits ist das ein enormer Sicherheitsgewinn beim Websurfen, allerdings verhindert diese Verschlüsselung auch, dass die Firewall die evtl. im verschlüsselten Datenstrom enthaltene Malware erkennen kann. Durch das HTTPs Scanning wird der Inhalt des Datenstroms bei Eintritt in die Firewall entschlüsselt und beim Austritt wieder verschlüsselt. Dadurch wird die Firewall in die Lage versetzt, den Datenstrom wieder auf Malware zu untersuchen.
Ausnahmen beim HTTPs Scanning sind Banking-Webseiten. Der Datenstrom beim Onlinebanking wird daher nicht auf Malware geprüft.
Dieses HTTPs Scanning kann auf Wunsch des Kunden ein- bzw. ausgeschaltet werden. DATIS aktiviert dieses Feature per Default.

URL-Filter

Der URL-Filter verhindert das Surfen auf Webseiten bestimmter Kategorien. Per Default werden folgende Kategorien durch den URL-Filter blockiert:
Drogen (Drugs)
Extremistische Seiten (Extremistic Sites)
Kriminelle Aktivitäten (Criminal Activities)
Nackte Haut (Nudity)
Verdächtig (Suspicious)
Waffen (Weapons)
und Webseiten deren Reputation schlechter als Verdächtig (Suspicious) ist.

FTP Malware Scanning

Verbindungen zu FTP-Server können über die Firewall (FTP-Proxy) abgesichert werden, so daß Dateien beim Hoch- bzw. Herunterladen auf Malware geprüft werden können.

Application Control

Bei aktiver Application Control werden die Datenströme, die durch die Firewall gehen, auf ihre Herkunft identifiziert. D.h. die Firewall kann erkennen, welcher Dienst diesen Datenstrom verursacht wie z.B. Facebook, Streaming, YouTube etc.
In der Lizenzierungsart Dediziert können individuelle Applikationen auf der Firewall gesperrt werden.

DATIS®

E-Mail Malware Scanning

Ein- und ausgehende E-Mails werden auf schädliche Anhänge geprüft und gegebenenfalls blockiert bzw. in Quarantäne gestellt.

E-Mail Antispam

Ein- und ausgehende E-Mails werden auf Spam geprüft und erhalten einen Spamscore. Erkannte Spammails werden im Betreff markiert und ab einem gewissen Spamscore auch in Quarantäne gesetzt. Zweimal täglich erhalten die Benutzer mit neuen Spammails in Quarantäne einen sogenannten Quarantänebericht, aus denen sie dann bestimmte Mails zustellen lassen können.

E-Mail Attachment-Filter

Passieren E-Mails mit Attachments die Firewall, werden die angehängten Dateien auf Dateiendung geprüft. Gehören die Dateien zu den nicht erlaubten Dateiendungen, werden diese Mails in Quarantäne gesetzt. Damit versucht man grundsätzlich erst einmal zu verhindern, dass ausführbare Dateien / Programme per E-Mail ins Unternehmen gelangen können und dort potentiell Schaden anrichten können. Ein Haupteinfallstor für Malware ist immer noch das Mediem E-Mail.
Folgende Dateiendungen sind per Default nicht erlaubt:
exe, msi, com, bat, vbx, hta, inf, js, jse, wsh, vbs, vbe, lnk, chm, pif, reg, scr, cmd, iso

E-Mail Real Time Blacklist

Ein wichtiger Bestandteil aller Antispam Techniken sind die sogenannten RBL (Real Time Blacklists). In diesen Listen werden IP-Adressen gepflegt, die beim Spamversand auffällig geworden sind. Damit versucht man sich vor Massenversendern von Spammails zu schützen.
Folgende RBLs werden per Default verwendet:
Commtouch IP Reputation (cyren.org) , cbl.abuseat.org, barracudacentral.org, bl.spamcop.net, zen.spamhaus.org

E-Mail Blacklist / Whitelist für Absender/Empfänger)

Es kommt leider immer noch sehr häufig vor, daß insbesondere kleine Unternehmen mit fehlerhafter E-Mailkonfiguration arbeiten. Es gibt ganz klare Richtlinien an die sich jeder Mailversender halten muss. Ansonsten läuft er Gefahr, daß seine Mails vom Empfänger abgelehnt werden.
Meist sind diese kleinen Unternehmen mangels eigener IT überfordert und letztlich bleibt nur der Weg, diese Absender in ein sogenanntes Whitelisting aufzunehmen. Trägt man einen Absender auf die Whitelist, werden seine E-Mails unabhängig von der Einhaltung der Mailrichtlinien angenommen.
Diese Ausnahmeregelung birgt allerdings viele Gefahren, denn Absenderadressen sind aufgrund der Beschaffenheit des Mailprotokolls sehr leicht zu fälschen.
Die Blacklist bewirkt genau das Gegenteil. Sie lehnt strikt alle E-Mails von diesen Absendern ab, die auf dieser Liste stehen. Gerne setzen Unternehmen Mailabsender von Spammails auf eine Blacklist in der Annahme, daß dadurch die Spammails von diesem Absender aufhören. Dies ist meist leider ein Trugschluß, da die Absenderadresse sehr dynamisch verwendet werden, so daß eigentlich ein Blacklisting keinen wirklichen Nutzen hat.
In der Lizenzierungsart DEDIZIERT haben Sie die Möglichkeit, diese White- und Blacklists nach Bedarf von DATIS pflegen zu lassen.

DATIS®

Mail-Empfang/-Versand über externen Provider (z.B. Strato,1&1, etc.)

Wird die Maildomain bei einem externen Provider gehostet, besteht die Möglichkeit, E-Mails vom Provider per POP3 abzuholen und per SMTP über ihn auch wieder zu versenden. Damit werden beim Mailversand auch alle Richtlinien für den Mailversand ordnungsgemäß eingehalten.
In der Lizenzierungsart BASIS ist dies die einzige Möglichkeit des Mail-Empfang/-Versand.
In der Lizenzierungsart SHARED ist dies zwar möglich, aber Malware-Scanning und Antispam-Funktionen werden dabei nicht aktiv.
In der Lizenzierungsart DEDIZIERT stehen Ihnen alle Varianten des Empfangs-/Versands inkl. Malware-Scanning und Antispam zur Verfügjung.

Mail-Empfang/-Versand direkt über MX-Record

Dies ist der direkte Web des Mail-Empfangs/-Versands ohne einen externen Provider. Alle Malware und Antispam-Funktionen stehen hier zur Verfügung, da die Firewall direkt mit dem Absender kommuniziert ohne Zwischenstation Provider. Sie haben hier die Möglichkeit, verschiedene Techniken zur Absicherung des Mailverkehrs zu verwenden wie z.B. DKIM, SPF-Record etc.
In der Lizenzierungsart SHARED teilen Sie sich die öffentlichen IP-Adresse (MX-Record) mit anderen DATIS-Kunden. Davon merken Sie im täglichen Betrieb allerdings nichts. Die Konfigurationen DKIM, SPF etc. teilen Sie sich ebenfalls mit anderen Kunden. Eine individuelle Konfiguration ist hier nicht möglich.
Im Shared Betrieb teilen Sie sich auch das Risiko des Blacklistings auf RBLs Listen mit anderen DATIS-Kunden. D.h. Ihr Dienst E-Mail könnte beeinträchtigt werden, obwohl Sie selbst nicht die Ursache für das Blacklisting waren.
Dieses Risiko haben Sie übrigens auch bei allen externen Providern, deren Mailserver wiederkehrend auf RBLs landenund damit der Mailverkehr beeinträchtigt wird.
In der Lizenzierungsart DEDIZIERT haben Sie hier eine eigene nur für Sie reservierte IP-Adresse. Die Konfiguration von DKIM, SPF und DMARC ist individuell möglich. Die Gefahr des Blacklistings ist zwar nicht vollständig gebannt, aber doch reduziert.

Mailverschlüsselung (s/Mime und PGP)

Ab der Lizenzierungsart DEDIZIERT kann die Firewall transparent E-Mailverschlüsselung und/oder Signierung mit den Technologien s/Mime und PGP durchführen. Dies passiert automatisch auf der Firewall bei durchgehendem Mailverkehr. Voraussetzung dafür ist, dass die notwendigen Keys zur Ver- und Entschlüsselung vorliegen und in die Firewall importiert wurden.
Dies ist eine schöne Möglichkeit, E-Mails per Default zu verschlüsseln, ohne dass der Endanwender mit Schlüsselfragen belästigt wird.
In allen niedrigeren Lizenzierungsarten können Sie lediglich Mailverschlüsselung auf Clientbasis nutzen.

Sandstorm Technology

Die Sandstorm Technology bietet einen erweiterten Schutz für bestimmte Dateitypen und Mailanhänge. Ausführbare Dateien und Dokumente mit ausführbaren Inhalten werden nicht nur mit den eingebauten Erkennungstechnologien sondern auch zusätzlich mit einer cloudbasierten Sandbox Technologie geprüft. Diese Technologie verspricht erweiterten Schutz vor gezielten Angriffen, Ransomware und Zero-Day-Bedrohungen durch Malware in Dateien.
Diese Technologie ist nur in der Lizenzierungsart DEDIZIERT möglich und ist separat zu erwerben.

DATIS®

Intrusion Prevention System
Das IPS prüft auf bekannte Angriffsmuster und verhindert diese. Zusätzliche schützt die Flood Protection gegen Denial-of-Service-Angriffe.

Advanced Threat Protection
ATP kombiniert mehrere Technologien, um ausgehenden Datenverkehr zu Command-and-Control-Hosts zu erkennen und zu sperren.

Web Server Protection (Application Firewall)
Die Web Server Protection härtet Webserver und Apps und stellt die Compliance über eine Web Applikation Firewall sicher. Sie verhindert Hackerangriffe, bei denen Techniken wie SQL-Injection, Cross Site Scripting, Directory Traversal und Cookie-Manipulationen angewandt werden.

Self-Service-Portal für Benutzer
Über ein Benutzerportal kann sich jeder Benutzer des Unternehmens an der Firewall anmelden und dort seine Mail-Quarantäne jederzeit bearbeiten und die Protokolle des Mailverkehrs einsehen.
Eine Zustellung einer Mail aus der Quarantäne kann jederzeit erfolgen und man muss nicht erst den Quarantänereport abwarten.

Protokollierung & Reporting
Die Firewall erzeugt regelmäßige Reports zu den Ereignissen und Datenverbindungen - das Morning Coffee Dashboard der Firewall in Form eines PDF-Reports.