

Ralf Nitzgen, Leiter Consulting ICC „SSL bietet nur scheinbar Sicherheit“

Über das Krypto-Protokoll Secure Sockets Layer (SSL) können gefährliche Inhalte am Virenschanner vorbei ins Unternehmen gelangen. Proxies ermöglichen die Virensuche in verschlüsselten Daten.

Das Secure-Socket-Layer-Protokoll ist beliebter denn je – und setzt zugleich Unternehmen unter Zugzwang. Immer mehr Anbieter wollen und müssen per SSL-Verschlüsselung die Integrität der Daten bei der Kommunikation zwischen ihren (potentiellen) Kunden und dem eigenen Web-Server garantieren. Doch SSL bietet nur eine scheinbare Sicherheit. Mit dem Protokoll schaffen sich Anwender ein anderes Sicherheitsproblem, das immer ärgerlicher wird: Gewöhnliche Schutzsysteme können bei solchen verschlüsselten Seiten nicht mehr feststellen, ob ein Virus ins System gelangt. Ein Mitarbeiter, der vom Arbeitsplatz aus eine Internetseite ansteuert, die SSL-verschlüsselt ist, setzt das Unternehmen demnach einem Sicherheitsrisiko aus.

Die Antwort vieler Anwender auf diese Gefahr lief bislang häufig darauf hinaus, dass sie einfach die Schotten dichtmachen: Weil die Sicherheit nicht garantiert werden kann, wenn verschlüsselte und damit nicht zu kontrollierende Inhalte bis zum PC eines Mitarbeiters gelangen, blockierten sie kurzerhand solche Seiten. Gab der Mitarbeiter eine entsprechende Web-Adresse ein, folgte eben die Meldung „Seite nicht gültig.“ Doch je mehr Seiten im Internet über SSL laufen, desto seltener lässt sich deren Nutzen verbieten.

Als immer weniger praktikabel erweist sich auch ein weiterer beliebter Versuch, das Problem in den Griff zu bekommen. Oft behelfen sich die IT-Leiter, indem sie die Verwendung von SSL-verschlüsselten Web-Seiten eigenhändig kontrollieren. Das bedeutet, jede einzelne Seite muss beim Administrator beantragt, von diesem geprüft und freigeschaltet werden. Solange sich die SSL-Verschlüsselung im Internet in Grenzen hielt, war das ein gangbarer Weg. Doch die Zunahme der SSL-Verschlüsselung hat den Administrationsaufwand erhöht, so dass andere Lösungen gefragt sind. Der Einsatz von SSL-Filtern stellt eine elegante Methode dar, verschlüsselte Web-Seiten für Mitarbeiter ohne Sicherheitseinbußen nutzbar zu machen. Solche Lösungen sind noch kein Massenphänomen, die Nachfrage steigt aber stetig an. Die Grundlage dieses Verfahrens ist dabei der Einsatz eines SSL-Proxys, der zwischen Firewall und Content-sowie Virenschanner geschaltet werden muss. So können alle eingehenden Daten entschlüsselt und kontrolliert werden. Danach werden sie erneut verschlüsselt und an den Endanwender weitergeleitet.

Diskreter Einsatz im Hintergrund

Der Mitarbeiter merkt dabei gar nicht, dass ein SSL-Proxy zwischen seinem Rechner und dem Web-Server aktiv ist. Er muss sich nicht einmal zusätzlich am Proxy anmelden, sondern kann wie gewohnt weitersurfen. Das Unternehmen ist gleichzeitig gegen den Missbrauch von Zertifikaten und gegen das Einschleppen von unerwünschten Inhalten über SSL geschützt. Ein SSL-Proxy arbeitet dabei nach dem Prinzip einer „Man-in-the-middle“-Attacke: Alle https-Anfragen der Arbeitsplatzrechner werden über den SSL-Proxy geleitet, der dann die Verbindung zum Ziel-Server herstellt. Beide Verbindungen werden verschlüsselt und kommen nur zustande, wenn der SSL-Proxy das Zertifikat des Ziel-Servers als gültig einstuft. Ist dies nicht der Fall, erhält der Anwender in seinem Browser-Fenster eine entsprechende Fehlermeldung. Wenn aber Verbindungen erfolgreich aufgebaut wurden, folgen die Antworten des Ziel-Servers. Auf einen verschlüsselten Datenverkehr vom Ziel-Server zum SSL-Proxy folgt der entschlüsselte Datenverkehr vom SSL-Proxy zum Virenschanner und zurück. Danach wird der Datenstrom wiederum verschlüsselt an die Arbeitsplatzrechner gesendet.

Die Installation des SSL-Proxy ist technisch gesehen einfach. Er wird in einer geschützten Zone installiert und in den https-Datenverkehr „eingeschleift“. Für die Virenprüfung wird ein Proxy-basierender http-Virenschanner verwendet, ein bereits vorhandener Virenschutz lässt sich aber auch benutzen. Dieser muss dann so konfiguriert werden, dass er seine Antworten an den SSL-Proxy sendet. Hat das Unternehmen weitere Proxies im Einsatz, sind auch diese so zu konfigurieren, dass der https-Datenverkehr über den SSL-Proxy läuft. Entscheidend ist die hohe Stabilität und Leistungsfähigkeit des SSL-Proxy. Je nach der zu erwartenden Last besteht die Möglichkeit, die Proxy-Hardware zu skalieren. Durch den Betrieb in einem Cluster (mit Load-Balancing und Failover) ist auch eine nachträgliche Anpassung möglich, indem weitere SSL-Proxys beziehungsweise Proxy-Ketten hinzugefügt werden.

Strenge Administration sichert Datenintegrität

Ein weitaus wichtigerer Aspekt ist organisatorischer Art. Anwender müssen beachten, dass beim Einsatz eines SSL-Proxys keine Ende-zu-Ende-Verschlüsselung mehr gegeben ist. Das erfordert besondere Maßnahmen. Sie betreffen die Zugangskontrolle zum Server-Raum ebenso wie die Einschränkung des Personenkreises für die Administration des SSL-Proxys. Außerdem müssen die Mitarbeiter des Unternehmens von dem SSL-Proxy unterrichtet werden. Denn es besteht die Möglichkeit, auf ihm oder dem Virenschanner vertrauliche Informationen auszuspionieren, da dort der Datenstrom unverschlüsselt ist.

Achillesferse SSL-Proxy und Virenschanner

Die Verbindungen zwischen dem Ziel-Server und dem SSL-Proxy sowie einem Arbeitsplatz und dem SSL-Proxy sind jeweils SSL-verschlüsselt. Daher ist schon systembedingt die Integrität der Daten auf diesen Strecken gewährleistet. Da die Kommunikation zwischen dem Virenschanner und dem SSL-Proxy aber unverschlüsselt erfolgen muss, ergeben sich hier mögliche Angriffspunkte. Diese lassen sich auf ein Minimum reduzieren, indem der SSL-Proxy und der Virenschanner auf derselben Hardware betrieben werden. In diesem Fall ist die unverschlüsselte Strecke auf diesen Server beschränkt. Es findet keine unverschlüsselte Kommunikation zwischen anderen Servern statt, so dass nicht durch Abfangen und Filtern des Datenstroms in der geschützten Zone die Integrität der Daten verletzt werden kann. Zum anderen hängt diese Integrität von der Vertrauenswürdigkeit der Administratoren, der Zugangskontrolle und dem sensiblen Umgang mit Passwörtern ab. Setzt ein Unternehmen diese Maßnahmen um, kann auch die Integrität des gesamten Datenstroms gewährleistet werden. Ein praktisches Beispiel ist der Einsatz der Lösung „TOMMY SSL-Proxy“ bei der Gmünder Ersatzkasse (GEK). Erst seit kurzem haben die 2000 Angestellten der fünftgrößten bundesweiten Krankenkasse die Möglichkeit, problemlos die SSL-verschlüsselte Web-Seiten aufzurufen. Dank des Proxys können sie jetzt direkt vom Arbeitsplatzrechner aus Internet-Apotheken nutzen, Schulen online buchen oder Online-Tracking-Systeme einsetzen. In der Vergangenheit wurden zu diesem Zweck nur einzelne Terminals freigeschaltet, die alle Mitarbeiter nutzen mussten. Die GEK hat mit der Implementierung des SSL-Proxys ein Problem gelöst, das immer mehr Unternehmen plagt. Jetzt kann die Krankenkasse den Datenverkehr im Unternehmen überprüfen, ohne der Zunahme von SSL-Seiten im Internet machtlos gegenüberzustehen.

Der Mitarbeiter merkt dabei gar nicht dass ein SSL-Proxy zwischen seinem Rechner und dem Web-Server aktiv ist. Er muss sich nicht einmal zusätzlich am Proxy anmelden, sondern kann wie gewohnt weitersurfen. Das Unternehmen ist gleichzeitig gegen den Missbrauch von Zertifikaten und gegen das Einschleppen von unerwünschten Inhalten über SSL geschützt. Ein SSL-Proxy arbeitet dabei nach dem Prinzip einer „Man-in-the-middle“-Angriff: Alle https-Anfragen der Arbeitsplatzrechner werden über den SSL-Proxy geleitet, der dann die Verbindung zum Ziel-Server herstellt. Beide Verbindungen werden verschlüsselt und kommen nur zustande, wenn der SSL-Proxy das Zertifikat des Ziel-Servers als gültig einstuft. Ist dies nicht der Fall, erhält der Anwender in seinem Browser-Fenster eine entsprechende Fehlermeldung. Wenn aber Verbindungen erfolgreich aufgebaut wurden, folgen die Antworten des Ziel-Servers. Auf einen verschlüsselten Datenverkehr vom Ziel-Server zum SSL-Proxy folgt der entschlüsselte Datenverkehr vom SSL-Proxy zum Virenschanner und zurück. Danach wird der Datenstrom wiederum verschlüsselt an die Arbeitsplatzrechner gesendet.

Die Installation des SSL-Proxy ist technisch gesehen einfach. Er wird in einer geschützten Zone installiert und in den https-Datenverkehr „eingeschleift“. Für die Virenprüfung wird ein Proxy-basierender http-Virenschanner verwendet, ein bereits vorhandener Virenschutz lässt sich aber auch benutzen. Dieser muss dann so konfiguriert werden, dass er seine Antworten an den SSL-Proxy sendet. Hat das Unternehmen weitere Proxies im Einsatz, sind auch diese so zu konfigurieren, dass der https-Datenverkehr über den SSL-Proxy läuft. Entscheidend ist die hohe Stabilität und Leistungsfähigkeit des SSL-Proxy. Je nach der zu erwartenden Last besteht die Möglichkeit, die Proxy-Hardware zu skalieren. Durch den Betrieb in einem Cluster (mit Load-Balancing und Failover) ist auch eine nachträgliche Anpassung möglich, indem weitere SSL-Proxys beziehungsweise Proxy-Ketten hinzugefügt werden.