Entschlüsseln mit Zscaler – das müssen Sie wissen

Frank Strecker Computer und Arbeit 4/2022 Ab Seite 16

Sicherheitssoftware Der Einsatz von Sicherheitssoftware ist zwar notwendig, darf aber nicht zur Totalüberwachung der Beschäftigten führen. Muss er auch nicht: Gängige Programme wie Zscaler Internet Access »ZIA« der Firma Zscaler bieten durchaus die Möglichkeit, Sicherheit und Beschäftigteninteressen in Ausgleich zu bringen. Wie das geht, verrät unser Autor.

Darum geht es

1. IT- und Datensicherheit sind wichtig zum Schutz des Unternehmens gegen äußere Bedrohungen.

2. Bei der Einführung von IT-Sicherheitssystemen haben Betriebs- und Personalräte mitzubestimmen.

3. Sie müssen darauf achten, dass keine lückenlose Überwachung der Beschäftigten entsteht.

Manchmal ist zu hören, es gebe keine Mitbestimmung in der IT-Sicherheit. Das ist falsch: Die Mitbestimmung greift auch hier, wenn Systeme eingeführt werden, die zur Verhaltenskontrolle im Sinne von § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) geeignet sind – und das ist bei IT-Sicherheitssystemen in der Regel der Fall. Unbestritten sind die IT- und Datensicherheit wichtig zum Schutz des Unternehmens gegen äußere Bedrohungen, und zwar für Arbeitgeber und Beschäftigte. Aber der gute Zweck rechtfertigt nicht jedes Mittel.

Zwischen Sicherheit und Überwachung

»Zero Trust«, die lückenlose Überwachung der IT-Systeme und Netzwerke, darf nicht zugleich die lückenlose Überwachung der Beschäftigten mit sich bringen. Es müssen alternative Mittel in Betracht gezogen und betroffene Interessen miteinander abgewogen werden. Betriebsräte dürfen sich also nicht

in die Ecke stellen lassen, wenn sie Sorgfalt und echte Beteiligung in diesem sensiblen Gebiet einfordern.

Die Überwachung der Beschäftigten muss begrenzt, erschwert und erkennbar gemacht werden. Ein Grundsatz der Videoüberwachung besagt: Zur Abwehr gegen äußere Bedrohungen dürfen keine Arbeitsplätze gefilmt werden. Um Kassenplätze und Schreibtische in Ladenräumen aus dem Bild zu nehmen, werden Bereiche der Kameralinse abgeklebt. Es ist nicht weltfremd, sich auch in der IT-Überwachung ähnliche Abklebungen zum Schutz der Beschäftigten gegen eine Komplettüberwachung auszubitten. Das Klebeband haben die Hersteller der Sicherheitslösung oft schon beigelegt, wie wir am Beispiel des häufig installierten Systems Zscaler Internet Access (ZIA) der Firma Zscaler aus San Jose, USA zeigen.

Was kann »ZIA«?

ZIA ist eine Kombination aus einem Virenscanner und einer Firewall in der Cloud, die verhindern soll, dass Risiken wie Viren oder andere Schadsoftware bis zum Endgerät der Benutzer:innen durchdringen. Die Konstruktion als weltweit vielfach vorhandener Cloud-Dienst ist leistungsfähiger als lokale Programme und verspricht, eine Schwachstelle zu beheben: Wenn nämlich Virenscanner erst auf dem Endgerät nach Gefahren suchen, kann sich dort (in seltenen Fällen) gerade bei der Durchsuchung Schadcode einnisten. Das Prinzip ist ähnlich wie beim Covid-Test an der frischen Luft, damit das Virus gar nicht ins Haus gebracht wird. Auf dem gesicherten Vorposten in der Cloud gibt es dieses Risiko nicht.

Wie lassen sich verschlüsselte Daten kontrollieren?

Weil Daten heute überwiegend verschlüsselt übertragen werden, können Sicherheitsprogramme wie ZIA sie nicht ohne Weiteres untersuchen: Man kann verschlüsselten Daten ihre Gefährlichkeit nämlich nicht ansehen. Es gibt kein Guckloch im Protokoll Transport Layer Security (TLS, teils noch als Secure Socket Layer, SSL, bekannt). Die Security am Flughafen kann verschlossene Koffer röntgen, bei verschlüsselten Datenpaketen ist das nicht möglich. Für eine Kontrolle müssen unverschlüsselte Daten im Klartext vorliegen.

Bleiben wir beim Bild mit dem Koffer: ZIA muss also den verschlossenen Koffer auspacken, um die Daten darin zu überprüfen. Am Flughafen gibt es dafür einen Generalschlüssel, im Internet aber nicht. Nur die vorgesehenen Empfänger selbst können ihre Datenpakete entschlüsseln. Technisch betrachtet ist die einzige Möglichkeit zum Kontrollieren eines mit SSL/TLS verschlüsselten Datenaustauschs, selbst zum Empfänger zu werden. Die Anfrage muss also unterbrochen und ein Mittelmann bzw. Relais auf dem Weg zum Server dazwischengeschaltet werden. So macht es auch ZIA: Es macht aus einem Koffer zwei und kontrolliert den Inhalt beim Umpacken. Technisch gesehen besteht also vom Endgerät zum ZIA-Vorposten und zurück eine verschlüsselte Verbindung, ZIA packt alles um in eine zweite verschlüsselte Verbindung zum Zielserver. Während des Umpackens kann ZIA in beiden Richtungen nach Gefahren suchen und ggf. Inhalte blockieren oder melden.

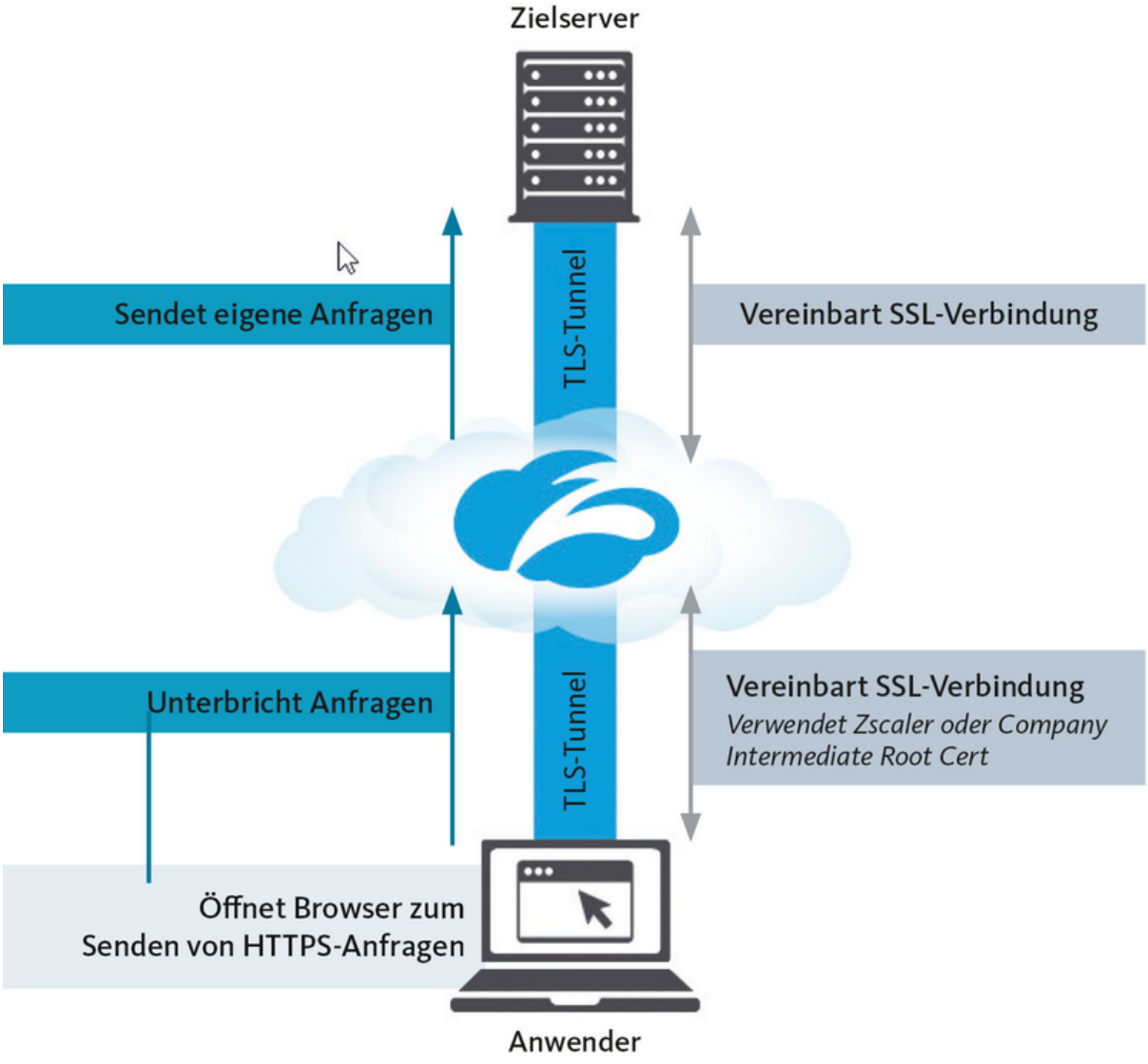
Übrigens: Weil eine SSL/TLS-Inspektion nur die Transportschicht entschlüsseln kann, bleibt eine erhöhte Vertraulichkeit auch beim Einsatz von ZIA machbar. Wer Inhalte besonders schützen will oder

muss, kann z. B. E-Mails mit S/Mime oder PGP schützen und Dateien noch vor dem Hochladen separat verschlüsseln, z. B. im Zip-Archiv.

Wie überwacht ZIA den Datenverkehr?

Selbstverständlich hat Zscaler auch Zugriff zur zentralen Steuerungsinstanz und spielt darüber die Regeln zur Erkennung von Schadcode ein, die es mit anderen Sicherheitsunternehmen zusammen pflegt. Zscaler lässt seine Kund:innen aber in einer zentralen Administrationsanwendung selbst steuern, wie ZIA sich für die jeweiligen Datenverbindungen verhalten soll. Unternehmensrichtlinien legen dann die Überprüfungen spezifisch für die jeweiligen Endgeräte und Endnutzer:innen fest. Gesteuert wird über:

1. Sperrlisten – wer darf welche Seiten und Apps aufrufen?
2. Bandbreitenüberwachung – welche Datenmenge Personen bzw. Geräte herunterladen oder hochladen dürfen
3. Datenverlustverhinderung/Data Loss Prevention (DLP) – Geschäftsgeheimnisse, die nicht ohne Weiteres hochgeladen werden, z. B. chemische Formeln, Kreditkartennummern
4. Risikovermeidung – welche Seiten werden nur mit Schutzmaßnahmen angezeigt?
5. SSL/TLS-Inspektion – welche Inhalte werden entschlüsselt und untersucht?



Welche Daten werden gespeichert?

Laut Zscaler erfolgt die Untersuchung auf Schadcode ohne dauerhafte Speicherung der Inhalte, gewissermaßen im Flug. Das scheint auch plausibel.

Für potenziell gefährliche Inhalte gibt es eine Möglichkeit zur kurzfristigen Zwischenspeicherung und Untersuchung durch die Benutzerin oder den Benutzer in einer sicheren Umgebung. Diese sogenannte »Cloud Browser Isolation« soll ausschließlich der betroffenen Person selbst zur Verfügung stehen, die Daten werden demzufolge nach Beenden der Sitzung gelöscht.

ZIA protokolliert aber die Benutzeraktivitäten mit Namen, Zeitangabe, IP-Adresse, den aufgerufenen Seiten sowie dem Verbindungserfolg und speichert diese für sechs Monate, wahlweise in Europa, USA oder den eigenen Rechenzentren der Kundschaft.

Die Benutzernamen können aus Berichten, Dashboards und Statistiken ausgeblendet oder in Datenexporten gegen 40-stellige Zufallszahlen ersetzt werden. In Verdachtsfällen kann man die Ausblendung bzw. Pseudonymisierung auch wieder aufheben.

Zscaler weist im Handbuch darauf hin, dass dies in manchen Regionen der Welt Vorschrift ist. Dazu gehört Europa. Allerdings müssten nach europäischem Datenschutzrecht auch die IP-Adresse und weitere Geräteinformationen ausgeblendet werden, weil die Administration daraus den Benutzer erkennen kann. Auch für diese Daten ist das Ausblenden in ZIA technisch möglich.

Was bedeutet eine Schnittstelle zum SIEM?

Zscaler kann alle genannten Protokolldaten zeitnah an ein zentrales Sicherheits-Informations- und Ereignis-Managementsystem (SIEM) des Kunden übertragen. Auch hierbei können Benutzerinformationen ausgeblendet werden – das geschieht aber nicht automatisch, »nur«, weil es für die Zscaler-Berichte ausgewählt wurde. Die Export-Schnittstelle vom ZIA zum SIEM ist sehr mächtig: Im SIEM kann sich in der Verbindung mit anderen Nutzungsdaten ein sehr genaues Bild der Aktivitäten der Beschäftigten ergeben. Die Weitergabe von Verbindungsdaten ins SIEM wird rechtlich für den Arbeitgeber besonders problematisch, wenn die private Nutzung der dienstlichen IT erlaubt oder geduldet ist und er als Telekommunikationsanbieter nach dem Tele-Kommunikations-Gesetz (TKG) gilt.

Woran Gremien denken müssen

Insgesamt sind die Protokolldaten das, worüber man sich beim Zscaler in Bezug auf Leistungskontrollen am meisten Sorgen machen muss, denn hier entsteht ein sehr detailreiches und genaues Bild der Beschäftigten, ein Weblogger, der bei der heutigen Bedeutung der Netzverbindung schon an die Wirkung eines Keyloggers auf früheren PCs heranreicht. Solche Keylogger hatte das Bundesarbeitsgericht (BAG) als unzulässige Totalüberwachung verbannt. Den Weblogger wird man nicht einfach aus der IT-Sicherheit verbannen können, weil er zur nachträglichen Ex-post-Analyse von Angriffsmechanismen notwendig ist. Das ist aber auch nicht notwendig, wenn der Einsatz der Weblogger gut geregelt wird.

Was Gremien beachten müssen:

- Gibt es eine klare Zweckbestimmung des Systems zur Abwehr äußerer Bedrohungen?
- Ist eine Nutzung der Daten für Leistungskontrollen rechtlich ausgeschlossen?
- Werden in den Protokollen die Benutzernamen und Geräteinformationen technisch ausgeblendet? Dürfen diese Daten nur bei Vorfällen auf Anfrage und mit Auditierung eingeblendet werden? (Hinweis: Auch bei der Weiterleitung von Protokolldaten an andere Systeme dürfen keine identifizierenden Informationen über Nutzer und Gerät im Klartext mitgesendet werden).
- Liegt eine gut verständliche Information für die Beschäftigten über die SSL-Inspektion und die Protokollierungen vor? (ggf. als Anlage aufnehmen)
- Wird sichergestellt, dass die Mitbestimmungsgremien unüberwacht kommunizieren können?
- Gibt es fragwürdige Unterschiede bei den Richtlinien für verschiedene Benutzergruppen?
- Was wird aus einer eventuell erlaubten oder geduldeten privaten Nutzung der dienstlichen IT? Erhalten die Beschäftigten einen Ausgleich für ihren Besitzstand, wenn diese abgeschafft wird?

Frank Strecker berät Gremien u. a. zur Personaldatenverarbeitung und zu Office 365.

www.tbs-nrw.de