Post vom Einbrecher

Alarmbildempfang per E-Mail

Zahlreiche Videoüberwachungssysteme bieten die Möglichkeit, im Alarmfall Bilder und Meldungen per E-Mail zu senden. Dies ist eine kostengünstige und herstellerneutrale Alternative zu den proprietären Verfahren, die eine spezielle Empfangssoftware des jeweiligen Geräteherstellers erfordern. Bei der Planung einer Videoüberwachungsanlage sind jedoch einige technische Grundlagen und daraus abgeleitete Regeln zu beachten, damit die Alarmbilder schnell und zuverlässig in der Leitstelle ankommen.

Von Hardo Naumann, Hannover

Viele Menschen nutzen E-Mail zur Kommunikation und verfügen über passende Empfangseinrichtungen. Die erforderliche Technik basiert auf offenen Standards, ist seit langem etabliert und weit verbreitet. Mit E-Mails können alle Arten von Daten übertragen werden. Daher liegt es nahe, auch Alarmbilder auf diese Weise zu übertragen.

Die Erfahrung lehrt jedoch:

- Es kann lange dauern, bis eine E-Mail ankommt
- E-Mails können auch ganz verloren gehen
- Stattdessen kommen viele E-Mails, die keiner haben möchte (Spam)
- Der Absender einer E-Mail ist nicht immer der, der im Briefkopf angegeben ist

Nur wenn man die Gründe dafür versteht, kann man Anlagen so planen und realisieren, dass diese Probleme vermieden werden.

Anforderungen

Für eine systematische Analyse werden die relevanten Aspekte unter folgenden Fachbegriffen zusammengefasst:

- **Authentizität**: Ist der Absender der E-Mail wirklich der, für den er sich ausgibt?
- **Vertraulichkeit**: Können Unbefugte die übertragenen Daten mitlesen?
- **Integrität**: Erhalte ich wirklich die Daten, die der Absender gesendet hat, oder wurden die Daten auf ihrem Weg manipuliert?
- **Verfügbarkeit**: Wie groß ist das Risiko, dass E-Mails durch technische Störungen, Fehlbedienung oder Eingriffe Unbefugter verloren gehen?
- **Latenz**: Wie lange dauert es vom Absenden der E-Mail bis der Empfänger sie wahrnimmt?

Die Technik zum Übertragen von E-Mails ist über viele Jahre gewachsen. In der Anfangszeit war der Kreis der Anwender klein und stammte vor allem aus dem wissenschaftlichen Bereich. Um eine zuverlässige und schnelle Kommunikation zu gewährleisten, wurden Verhaltensregeln verabredet, die so genannte „Netiquette“: Es lag in der Verantwortung jedes Teilnehmers, selbst auf die Einhaltung der Regeln zu achten - das hat seinerzeit gut funktioniert.

Mit dem rasanten Wachstum des Internets wurde der Kreis der Anwender immer größer, unübersichtlicher und damit auch anonymer; die Inhalte wurden immer stärker von kommerziellen Interessen geprägt. Inzwischen sind über 90% aller verschickten E-Mails Spam, also von den Empfängern nicht erwünschte Werbesendungen. Bei der Planung einer Datenverbindung über das Internet muss vom „worst case“ ausgegangen werden: Alles, was technisch möglich ist, wird irgend jemand zum Missbrauch nutzen.

Ausgangslage

Wenn man keine besonderen Vorkehrungen trifft, werden E-Mails ungesichert durch das Internet transportiert. Unbefugte könnten die E-Mails lesen und manipulieren. Deshalb wurden technische Verfahren entwickelt, die davor schützen, z.B. GPG – in der Praxis werden diese Verfahren jedoch aus Unkenntnis oder mangelndem Problembewusstsein nur selten verwendet.

Abbildung 1 zeigt die an einer E-Mail Übertragung beteiligten Komponenten. Die E-Mail wird von einer zur nächsten Komponente weitergereicht. Die Gesamt-Laufzeit (Latenz) einer E-Mail ergibt sich daher als Summe der Verzögerungen der einzelnen Komponenten.

Im Mail-Client des Senders sind die Zugangsdaten des zugehörigen Mail-Servers konfiguriert. Als Übertragungsprotokoll vom Sender zu seinem Mail-Server und zwischen den Mail-Servern wird meist SMTP verwendet (siehe Stichwortbox). Aus dem Domain-Teil der E-Mail-Adresse (alles, was hinter dem @-Zeichen steht) ermittelt der Mail-Server auf Senderseite mit Hilfe des DNS die IP-Adresse des passenden Mail-Servers für den Empfänger und überträgt die E-Mail dorthin. Von dort ruft der Mail-Client des Empfängers die E-Mail üblicherweise mit den Protokollen IMAP oder POP3 ab.

Damit sich eine Komponente mit der nächsten verbinden kann, benötigt sie deren IP-Adresse. Oft wird nicht die IP-Adresse selbst, sondern ein so genannter DNS-Name angegeben, beispielsweise *mail.gmx.net* für den Mail-Server der Firma GMX. DNS-Namen haben gegenüber IP-Adressen neben der besseren Lesbarkeit den Vorteil, dass sie

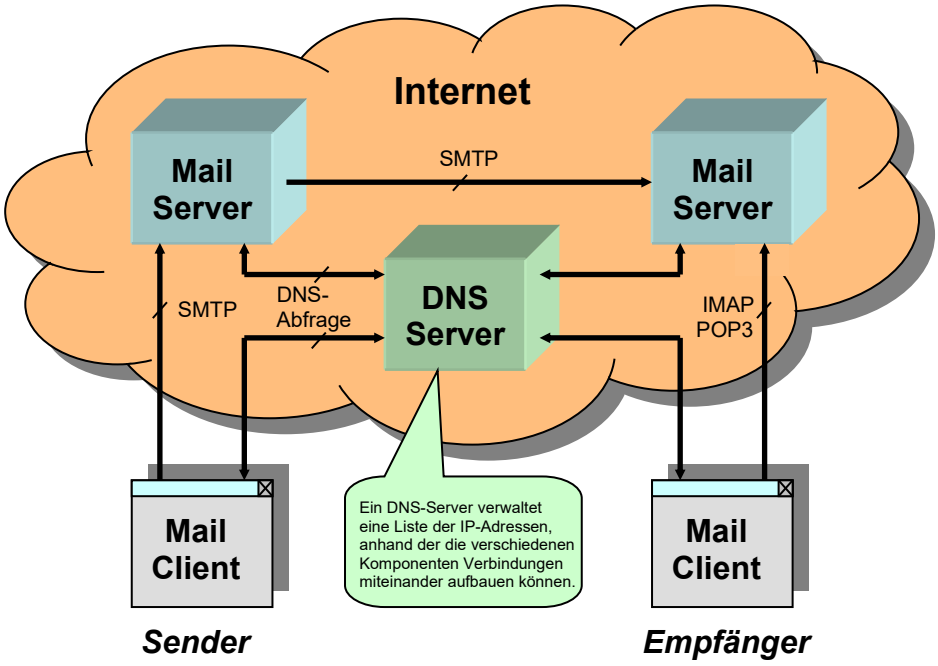

Abb. 1: E-Mail Übertragung über das Internet - vereinfachte Darstellung der beteiligten Komponenten

dynamische IP-Adressen erlauben, also Netzwerkanschlüsse, deren IP-Adresse sich im Laufe der Zeit ändert. Jede Komponente, bei der ein Name in dieser Form konfiguriert ist, muss zunächst eine Anfrage an das Domain Name System (DNS) stellen, um die zugehörige IP-Adresse zu erhalten. Das DNS ist ein Internet-Dienst, der eine Liste aller DNS-Namen und der zugehörigen IP-Adressen verwaltet, anhand der er die gewünschten Daten ermitteln und bereitstellen kann. Wenn sich bei einem Netzwerkanschluss die IP-Adresse geändert hat, kann es einige Minuten dauern, bis die neue Adresse im DNS eingetragen ist. So lange ist die betreffende Komponente via DNS-Namen nicht erreichbar. Wenn es auf hohe Geschwindigkeit und ununterbrochene Verfügbarkeit ankommt, sollten daher feste IP-Adressen verwendet und direkt konfiguriert werden.

Der nächste Faktor, der die Latenz beeinflusst, ist die Netzwerkverbindung zwischen den Komponenten. Die Technik wird zwar immer leistungsfähiger, aber auch das Datenaufkommen wächst weiter, bei E-Mails zum größten Teil durch Spam.

E-Mails werden im Mail-Server zwischengespeichert und erst dann weitergeleitet, wenn der Server die vorangegangenen Aufträge abgearbeitet hat. Viele Mail-Server wenden heute komplexe Filtermechanismen an, um Spam auszusortieren. Dies erfordert viel Rechenzeit, so dass es je nach Anzahl und Größe der eintreffenden E-Mails unterschiedlich lange dauern kann, bis eine E-Mail weitergeleitet wird.

Die letzte Verzögerung bei der Übertragung von E-Mails resultiert daraus, dass der Mail-Client des Empfängers nur in bestimmten Intervallen bei seinem Mail-Server nachfragt, ob neue Post eingetroffen ist; zwischenzeitlich eintreffende Post wird erst im nächsten Abfrageintervall angezeigt.

bzw. Verschlüsselung mit SSL/TLS vor Auslesen und Veränderungen geschützt.

Die E-Mail-Adressen in solchen geschlossenen Systemen können frei gewählt werden; sie müssen nur bei Absender und Empfänger übereinstimmend konfiguriert werden. Zur besseren Unterscheidung von öffentlichen E-Mail-Adressen sollte die Pseudo-Top-Level-Domain *.local* verwendet werden. Die Bildquelle 3 bekommt dann beispielsweise die Adresse *bq3@ebues.local* und sendet ihre Alarmdaten an *alarmserver@ebues.local*.

Für kurze Reaktionszeiten ist es entscheidend, dass die E-Mails nicht über mehrere Stationen weitergereicht, sondern direkt in die Leitstelle gesendet und dort unmittelbar gemeldet werden. Dazu muss in der Leitstelle ein spezieller SMTP-Server eingerichtet werden, der die in der E-Mail enthaltenen Daten (Bilder, Texte) auspackt und auf einem File-Server in geeigneten Standardformaten (JPEG, ASCII) speichert, damit sie von dort aus in der Leitstelle weiter verarbeitet werden können (Abbildung 2). Das leistet z.B. der AlarmReceiver SMTP der Firma Accellence Technologies [1]. Ein Alarm-Server überwacht die Verzeichnisse des File-Servers und meldet eintreffende Alarmdaten unverzüglich an die Arbeitsplätze in der Leitstelle.

Da die Bildquelle via SMTP direkt mit dem Mail-Server in der Leitstelle verbunden ist, erhält sie auch Rückmeldungen aus der Leitstelle, ob die Alarmdaten dort angekommen sind. Eine Datenübertragung mit SMTP ist aufgrund seiner Beschränkung auf Textzeichen (es werden nur 7 Bit jedes Bytes genutzt, Binärdaten werden mittels Base64 codiert) geringfügig langsamer gegenüber optimierten Binärformaten, hat dafür aber den Vorteil eines offenen Standards und seiner weiten Verbreitung.

Die Funktionsweise von SMTP

SMTP steht als Abkürzung für „Simple Mail Transfer Protocol“, auf Deutsch „Einfaches Protokoll zum Übertragen von Post“. Dieses Protokoll ist weit verbreitet, um Daten von einem Programm auf dem PC des Anwenders (Mail-Client) zur zentralen elektronischen Poststelle (Mail-Server) zu senden.

Ein Protokoll regelt in der Informationstechnik den Ablauf, nach dem verschiedene Teilnehmer Daten miteinander austauschen. SMTP ist ein textbasiertes Protokoll, die übertragenen Zeichen sind somit für Menschen lesbar. Ein kleiner Ausschnitt aus einer SMTP-Sitzung macht das Prinzip deutlich:

HELO
250 mail.gmx.net GMX Mailservices
MAIL FROM: <hardo.naumann@gmx.de>
250 ok
RCPT TO: <naumann@accellence.de>
250 ok
DATA
354 Go ahead

In der ersten Zeile begrüßt der Client den Server mit „Hallo“, wie in der Informationstechnik üblich auf Englisch und leicht verkürzt. Der Server antwortet mit Nennung seines Namens. Daraufhin teilt der Client seine Absenderadresse (MAIL FROM) und zwei Zeilen später die gewünschte Empfängeradresse (RCPT TO) der E-Mail mit, der Server bestätigt jeweils mit OK. Schließlich sagt der Client, dass nun der Inhalt der E-Mail kommt (DATA). Der Server fordert dazu auf, mit dem Senden der Daten zu beginnen.

Der Server stellt seinen Antworten einen 3-stelligen Zahlencode voran, an dem der Client erkennen kann, ob der vorherige Schritt erfolgreich ausgeführt wurde. SMTP wurde 1982 definiert und 1995 erweitert (ESMTP), das grundlegende Prinzip gilt weiterhin.

Bei geeigneter Auslegung des Systems lassen sich Alarm-Meldezeiten unterhalb einer Sekunde realisieren. Durch parallelen Betrieb eines Testalarm-Generators kann die Funktion der gesamten Alarm-Übertragungsstrecke laufend überwacht werden. Damit steht einer Alarmbildübertragung per E-Mail nichts mehr im Weg.

Lösung

Alle beschriebenen Probleme lassen sich lösen, indem E-Mails mit Alarmdaten nicht öffentlich über das Internet übertragen werden, sondern ausschließlich verschlüsselt und direkt. Das Internet dient dabei nur als physikalisches Medium („Leitung“) zur Fernübertragung der Daten; auf die Verwendung öffentlich zugänglicher Mail- und DNS-Server wird bewusst verzichtet. Nur Sender mit gültiger Authentifizierung für VPN oder Verschlüsselung (SSL/TLS) können überhaupt Alarmdaten an die Leitstelle senden. Die Daten werden dabei durch den VPN-Tunnel

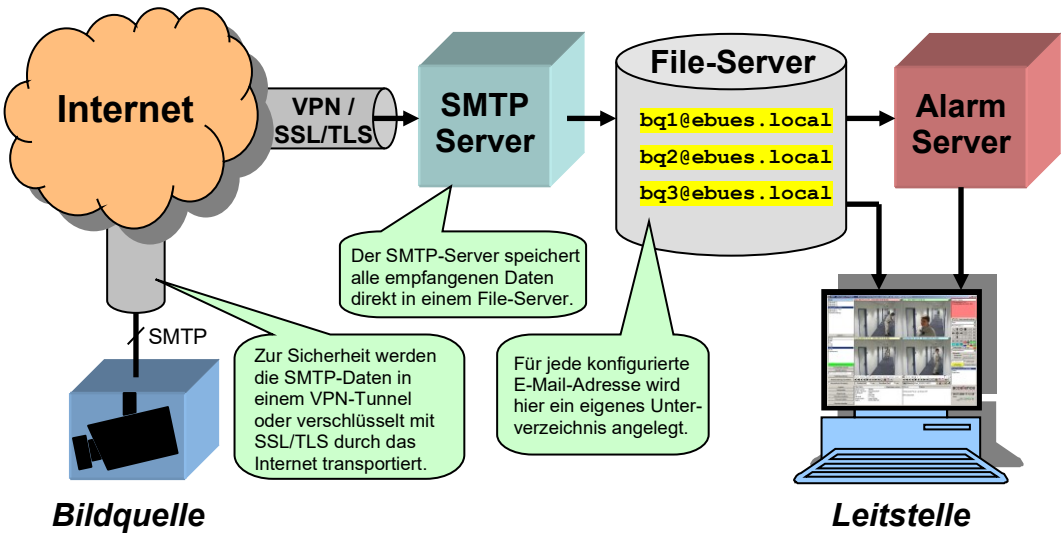

Abbildung 2: Sichere Alarmbild-Übertragung mit SMTP, verschlüsselt und direkt in die Leitstelle

Quellen / weiterführende Informationen: [1] https://www.ebues.de/AccAlarmReceiverSMTP.pdf