arago

Institut für komplexes
Datenmanagement AG

IT-Sicherheit

Angriffs- und Schadensszenarien bei mittelständischen Unternehmen

Inhalt

Verlust / Veränderung/ Ausspähen von Daten, rechtliche Probleme durch Verletzung des Datenschutzes

Zugriff auf ungeschützte Dateifreigaben über das Netzwerk

Ein Unternehmer hat die PCs in seinem Büro vernetzt, jeder Mitarbeiter soll auf die Dateien der anderen PCs zugreifen können. Er richtet einen Internetzugang per ISDN an einem der PCs ein. Der Internetzugang erfolg über einen normalen Internetprovider, bei dem keine kundenspezifische Firewall existiert.

Auf den PCs existieren die Standard-Dateifreigaben von Windows – aus dem Internet kann ohne Einsatz zusätzlicher Tools problemlos auf die PCs des Unternehmers zugegriffen werde: Dateien können gelesen, kopiert, verändert und gelöscht werden, ohne dass dies auffallen würde.

- Hierbei handelt es sich um einen Netzwerkangriff, der durch die arago Security-Komponente „Firewall“ vermieden werden kann.

Verlust / Veränderung/ Ausspähen von Daten, rechtliche Probleme durch Verletzung des Datenschutzes

Gezieltes Stehlen von Dateien, Berechnungen, Plänen, …

Alle Serverdienste stehen in einem ungeschützten, mit dem Internet verbundenen LAN auch unerwünschten Benutzern offen: Sowohl der Konkurrent aus dem Nachbarort, als auch der unbekannte Wirtschaftsspion aus Fernost erhalten ihre Informationen ohne technischen Aufwand - sei es bei gezielter Suche oder als Zufallstreffer.

Das Angebot der Konkurrenzfirma war nur wenige Euro billiger, schon das war kein Zufall, der Auftrag bei diesem lukrativen Projekt ging aber auch deswegen verloren, weil aus dem Nichts die schlechte Bilanz aus dem Vorjahr an den Auftraggeber gelangt war ...

- Hierbei handelt es sich um einen Netzwerkangriff, der durch die arago Security-Komponente „Firewall“ vermieden werden kann.

Verlust / Veränderung/ Ausspähen von Daten, rechtliche Probleme durch Verletzung des Datenschutzes

Ausspionieren und Stehlen von Zugangsberechtigungen

Der Schutz von Passwörtern in Ihrem Haus war Ihnen schon immer besonders wichtig, damit Unbefugte nicht an Ihre Daten herankönnen. Und davon gibt es in einem grossen Metallbetrieb doch eine ganze Reihe: Lieferanten, externe Firmen, Fahrer, Aushilfen...

Leider haben Sie übersehen, dass es durch Einbruch in Ihr Netz über den ungeschützten Internetzugang Dritten möglich war, all diese Zugänge zu stehlen. Jeder Fahrer auf dem Hof könnte jetzt in einem unbeobachteten Augenblick ihre Lohnbuchhaltung einsehen.

- Hierbei handelt es sich um einen Netzwerkangriff, der durch die arago Security-Komponente „Firewall“ vermieden werden kann.

Verlust / Veränderung/ Ausspähen von Daten, rechtliche Probleme durch Verletzung des Datenschutzes

Ausspähen von Verbindungen und Datentransfers

Ein Unternehmen überträgt jeden Tag die aktuellen CNC-Daten ihrer Produkte über das Internet unverschlüsselt, ohne VPN, zu einer Partnerfirma, welche die Fertigung übernommen hat.

Ein Konkurrent aus dem Ausland hat dies herausgefunden. Seit Monaten schneidet er die Daten schon mit. Die Plagiate aus Fernost sind von hoher Qualität, schon bald sinkt der Umsatz, die teure Entwicklungsabteilung muss verkleinert werden.

- Hierbei handelt es sich um ein Sicherheitsproblem wegen unverschlüsselter Datenkommunikation über das Internet, der durch die arago Security-Komponente „VPN“ vermieden werden kann.

Verlust / Veränderung/ Ausspähen von Daten, rechtliche Probleme durch Verletzung des Datenschutzes

Diebstahl von Kundendaten

Die Firma speichert ihre Kundendaten in einer zentralen Datenbank im LAN. Das Unternehmen ist im Sanitätsbereich auf ein besonderes Krankheitsbild spezialisiert.

Da das Unternehmensnetzwerk mit dem Internet ohne Firewall verbunden ist und der Datenbankrechner ein Standardpasswort hat, erlangen Jugendliche Zugang zu den Kundendaten. Sie machen sich einen Spass daraus, die Kunden mit Mails wegen ihrer etwas unappetitlichen Krankheit zu verspotten. Der Anwalt eines der betroffenen Patienten ermittelt den Zusammenhang...

- Hierbei handelt es sich um einen Netzwerkangriff, der durch die arago Security-Komponente „Firewall“ vermieden werden kann.

Verlust / Veränderung/ Ausspähen von Daten, rechtliche Probleme durch Verletzung des Datenschutzes

Entscheidende und strategische Informationen werden unkontrolliert versendet und deren Sicherheit ist gar nicht überschaubar

Der Geschäftsführer einer mittelständischen Firma ist viel im In- und Ausland unterwegs, sein Notebook und sein Mobiltelefon hat er immer dabei. Für wichtige Entscheidungen ist er immer erreichbar, per Fax, per Telefon, per eMail. Einen Firmendial-In oder verschlüsselte Kommunikation (VPN o.ä.) wurde aus Kostengründen nicht implementiert. Besonders wichtige Verträge mailt die Sekretärin ihm auf seinen WebMail-Account.

Von dort kann er sie aus dem Hotel oder aus dem Internetcafe downloaden – leider sind diese Daten aber nicht nur für den Geschäftsführer lesbar. Möglicherweise sind die Vertragsinhalte bereits bei Dritten, für die sie nicht bestimmt waren... Oder nehmen wir ein ähnliches Prozedere im juristischen Bereich – der gegnerische Anwalt weiß jeden Schritt des Syndikus im Voraus ...

- Hierbei handelt es sich ein Sicherheitsproblem wegen unverschlüsselter Datenkommunikation über das Internet, das durch die arago Security-Komponente „VPN“ vermieden werden kann.

Verlust / Veränderung/ Ausspähen von Daten, rechtliche Probleme durch Verletzung des Datenschutzes

Zufälliger Versand vertraulicher Informationen

Ein eMail-Wurm hat PCs in Ihrem Unternehmen befallen. Er verschickt sich zur Weiterverbreitung an alle Adressaten in Ihrem eMail-Adressbuch. Dabei hängt er zufällig ausgewählte Office-Dateien von Ihren PCs an die Mails an: Abrechnungen, Bilanzen, Besprechungsprotokolle aus einer Krisensitzung, Preiskalkulationen...

Besonders ärgerlich: In Ihrem email-Adressbuch befinden sich die Adressen von Kunden, Partnern, Konkurrenten, Lieferanten, Banken...

- Hierbei handelt es sich um einen Angriff per eMail, der durch die arago Security-Komponente „Contentsecurity / Mailvirenscanner“ abgewehrt werden kann.

Verlust / Veränderung/ Ausspähen von Daten, rechtliche Probleme durch Verletzung des Datenschutzes

Gezieltes Ausspionieren vertraulicher Informationen

Ein Trojaner wird per eMail an verschiedene Empfänger verschickt. Auf den PCs dieser Personen wird er nach dem Öffnen der Mail unbemerkt aktiv, sammelt nach einem definierten Muster Daten ein und verschickt diese per eMail oder auf anderem Wege an einen unbekannten Empfänger im Internet.

- Hierbei handelt es sich um einen Angriff per eMail, der durch die arago Security-Komponente „Contentsecurity / Mailvirenscanner“ abgewehrt werden kann.

Missbrauch von Systemen: rechtliche Risiken und Kostenverursachung

Missbräuchliche Nutzung von Ressourcen

Ein Unternehmen hat PCs, die mit dem Internet verbunden sind. Diese sind nicht durch eine Firewall gesichert. Dritte verschaffen sich Zugang zu einem der Server-PCs und verwenden diesen missbräuchlich als Fileserver für eine öffentliche Tauschbörse im Internet, auf der Raubkopien und Bilder vertrieben werden.

Die Performance des Firmennetzes bricht zusammen, obwohl niemand dort Arbeitet. Ein Unternehmen der Musikindustrie erhebt Klage wegen des Betriebs einer illegalen Tauschbörse gegen den Eigner des Systems...

- Hierbei handelt es sich um einen Netzwerkangriff, der durch die arago Security-Komponente „Firewall“ vermieden werden kann.

Missbrauch von Systemen: rechtliche Risiken und Kostenverursachung

Kostenverursachung durch Systemkompromittierung

Eine Firma betreibt in ihrem ungesicherten Netz einen zentralen Faxserver zur Vereinfachung von Arbeitsabläufen. Dritte verschaffen sich Zugang zum Netz und versenden eine große Anzahl von Werbefaxen an die im Adressbuch hinterlegten Kunden oder an sogenannte „Mehrwertnummern“.

Neben den verärgerten Kunden muss der Unternehmer zudem die Telefonkosten tragen, besonders im zweiten Fall eine ärgerliche Aufgabe...

- Hierbei handelt es sich um einen Netzwerkangriff, der durch die arago Security-Komponente „Firewall“ vermieden werden kann.

Missbrauch von Systemen: rechtliche Risiken und Kostenverursachung

Unbemerkte Fernsteuerung des Arbeitsplatzes

Der Meister des Unternehmens hat sich zur Vereinfachung seines Arbeitsablaufes ein kostenloses Tool aus dem Internet heruntergeladen. Es ist ihm nicht bewusst, dass es sich hierbei um einen Trojaner handelt, der den PC über das Netz fernsteuerbar macht – sogar das Monitorbild kann mitgelesen werden.

Der eingesetzte Desktop-Virenscanner erkennt diesen Trojaner im installierten Zustand nicht, der er als Windows-Dienst läuft, ein Web-Virenscanner zum Schutz beim Download existiert nicht.

- Hierbei handelt es sich um einen Angriff per Web, der durch die arago Security-Komponente „Contentsecurity / Webvirenscanner“ abgewehrt werden kann.

Missbrauch von Systemen: rechtliche Risiken und Kostenverursachung

Kostenverursachung, Missbrauch und das Unbrauchbarmachen von Arbeitsplätzen

Durch den Besuch einer Webseite ohne Web-Contentscanner wurde ein sogenannter „0190-Dialer“ auf dem PC eines Mitarbeiters installiert. Seitdem wählte dieser Rechner über das Modem unbemerkt teure 0190-Rufnummern an.

Es entstanden Telefonkosten in Höhe von mehreren tausend Euro, bevor der Dialer durch Zufall entdeckt wird. Der lokale Virenscanner konnte das Programm nicht erkennen.

- Hierbei handelt es sich um einen Angriff per Web, der durch die arago Security-Komponente „Contentsecurity / Webvirenscanner“ abgewehrt werden kann.

Sabotage und Beeinträchtigung des Produktionsbetriebs

Zerstörung des Netzzugangs durch Überlastung

Die PCs eines Unternehmens sind untereinander vernetzt. Der Zugang zum Internet ist für Information und Einkauf notwendig. Preislisten und Lagerbestände werden mit den Großhändlern online abgeglichen. Aus Kostengründen wurde das Netz nicht besonders abgesichert, im Computersystem des Unternehmen gibt es „nichts zu stehlen“. Durch einen sogenannten „Internetwurm“, der seit einigen Tagen im Umlauf ist, werden PC-Systeme mit dem Betriebssystem Windows XP, infiziert. Das System muss dafür nur aus dem Internet erreichbar sein. Jedes infizierte System infiziert dann in einer Art Kettenreaktion weitere Rechner.

Die Arbeit Im Unternehmen bricht nicht nur zusammen, weil die PCs innerhalb weniger Stunden komplett infiziert sind. Die PCs bauen in dem Versuch, weitere Systeme zu infizieren, so viele Verbindungen in die Welt auf, dass der Netzzugang nach kurzer Zeit zusammenbricht.

- Hierbei handelt es sich um einen Netzwerkangriff, der durch die arago Security-Komponente „Firewall“ vermieden werden kann.

Sabotage und Beeinträchtigung des Produktionsbetriebs

EDV Ausfälle durch Virenbefall

Eine Mitarbeiterin in einer Firma, die ihr LAN mit einer Firewall abgesichert hat, empfängt eine eMail von einer Partnerfirma. Als Anhang enthält die Mail eine Word-Datei mit einem Macro. Vom Absender unbemerkt ist das Dokument mit einem Macro-Virus infiziert.

Dieser verbreitet sich mit hoher Geschwindigkeit auf den PCs der Firma, als die Mitarbeiterin das Dokument öffnet. Der PC-Betreuer braucht einige Tage, bis in der Firma wieder normal gearbeitet werden kann.

- Hierbei handelt es sich um einen Angriff per eMail, der durch die arago Security-Komponente „Contentsecurity / Mailvirenscanner“ abgewehrt werden kann.

Sabotage und Beeinträchtigung des Produktionsbetriebs

Datenverlust oder Datenverfälschung durch Virenbefall

Ein per eMail eingeschlepptes Computervirus löscht alle Dateien im Laufwerk c:\ des Sekretariats-PCs. Weitere PCs, auch in der Konstruktion, sind befallen. Dort werden ganze Festplatten gelöscht, bevor auf den anderen PCs die aktuellste Version des Desktop-Virenscanners aktiv wird.

Am Tag nach dem Vorfall weiß der Leiter des Konstruktionsbüros noch nicht, welche Aufträge er noch erfüllen kann und bei welchen er die kompletten Unterlagen neu erstellen lassen muss...

- Hierbei handelt es sich um einen Angriff per email, der durch die arago Security-Komponente „Contentsecurity / Mailvirenscanner“ abgewehrt werden kann.

Sabotage und Beeinträchtigung des Produktionsbetriebs

Überlastung des eMail Systems und damit nicht Verfügbarkeit des Systems

Ein eMail-Virus verbreitet sich im Internet mit rasender Geschwindigkeit. Auch einige PCs im Unternehmen sind betroffen. Obwohl die Infektion weiterer PCs verhindert werden konnte, ist eine normale Büroarbeit nicht möglich:

Das Virus verschickt sich selbst mehrere hundert mal pro Sekunde an neue Empfänger, dadurch wird das eMail-System im Unternehmen überlastet und bricht zusammen.

- Hierbei handelt es sich um einen Angriff per email, der durch die arago Security-Komponente „Contentsecurity / Mailvirenscanner“ abgewehrt werden kann.

Sabotage und Beeinträchtigung des Produktionsbetriebs

Einschleppen von Viren auf den Arbeitsplatz

Ein Praktikant lädt eine Spielesoftware von einer zweifelhaften Internetseite herunter und installiert sie auf einem PC im Büro. Da er sich nicht sicher ist, ob der lokal installierte Virenscanner auch bei Spielen anschlägt, hat er diesen zur Vorsicht deaktiviert.

Da am Internetgateway der Firma nicht auf Viren gescannt wird, hat das Virus sich bereits weit verbreitet, als der Desktop-Virenscanner auf dem PC eines Kollegen Alarm schlägt...

- Hierbei handelt es sich um einen Angriff per Web, der durch die arago Security-Komponente „Contentsecurity / Webvirenscanner“ abgewehrt werden kann.

Inhalt

Verringertes Risiko mit einem Packet Filter

- Es können keine Netzangriffe erfolgen, dies schützt vor den meisten obigen Szenarien in Bezug auf Datenverlust, unberechtigten Zugriff...
- Ein zentraler Netzzugang ist Voraussetzung für kontrollierten Web- und eMail Verkehr.
- Kostenverminderung bei der Pflege der einzelnen Systeme
- Kontrolle des Verkehrs von innen nach außen – selbst eingeschleppten Würmern und Trojanern wird die Kommunikation verwehrt.

Verringertes Risiko mit Content Security

- Minimierung von einfallenden Viren und Trojanern
- Risikobehaftete Inhalte können komplett gefiltert werden.
- Wenn Content Security auch für Web betrieben wird, kann der eMail Virenschutz nicht durch Web Mailer umgangen werden.
- Dialer und andere Kostenverursacher werden, bevor sie einen Arbeitsplatz erreichen, ausgeschaltet.

Zusätzlich verringertes Risiko mit Content Security und eigener Hardware

- Keine Performance Probleme.
- Getrennte Betrachtung von Inhalten und Netzwerk.
- Anfälligkeit für Komplettausfälle durch Überlastung minimiert.
- Das Content Security System ist nicht aus dem Internet angreifbar und kann daher nicht umgangen werden.

Verringertes Risiko mit einem VPN

- Kein Diebstahl von Daten, wenn ein Mitarbeiter diese ins Unternehmen übermittelt.
- Keine unsicheren Zugänge in und aus dem Unternehmen, die alle anderen Sicherheitsmaßnahmen umgehen und kompromittieren können.
- Senkung von Verbindungskosten.
- Direkter Zugriff auf interne Ressourcen – nicht zwei Arbeitsplätze oder zwei IT-Umgebungen, je nachdem ob ein Mitarbeiter intern oder extern ist.

Inhalt

Alternativen und ihre Nachteile - Zentrale Firewall beim Internetprovider

- Viele Unternehmen entscheiden sich statt für eine eigene Firewall, wie sie von arago angeboten wird, für eine zentrale Firewall bei ihrem Internetprovider. Sie kaufen also, wie sie meinen, einen sicheren Internetzugang aus einer Hand.

- Diese Lösung schützt zwar vor einfachen Angriffen, kann aber in keinem Fall eine individuelle Sicherheit bieten. In der Regel ist den einzelnen Kunden nicht transparent, was für Regelsätze auf der Providerfirewall aktiv sind. Durch Konfigurationswünsche eines anderen Kunden kann die Sicherheit der Firewall kompromittiert werden.

- Die Performance einer solchen Firewall wird generell geteilt: Verursacht ein anderer Kunde hohe Last, kann hiergegen nichts unternommen werden.

- Ein kundenindividuelles Reporting und damit eine Nachvollziehbarkeit der Angriffe erfolgt in der Regel nicht. Zudem erfordert eine Providerfirewall das Vertrauen, dass die Strecke zwischen Provider und Kunde sicher ist... was sie a priori nicht sein kann.

- Zusätzliche Funktionen wie Content-Security, VPN oder die hohen Verfügbarkeiten und individuellen Supportmöglichkeiten der arago WebFarm bleiben ohnehin außen vor.

Alternativen und ihre Nachteile – Sicherheitslösung bei einem anderen Anbieter

- Oft werden Sicherheitslösungen auch in Einzelangeboten zusammengestellt. Wenn man diese richtig einsetzen will, muss man selbst das gesamte Security Know-How haben.

- Wenn ein Software- oder Hardwarehersteller eine Lösung anbietet, dann ist diese auf sein Produkt ausgelegt. Wenn dieses Produkt eine Sicherheitslücke hat, gibt es keine Alternativen.

- Management und Support werden oft nicht 24/7 angeboten. Dies ist aber wichtig, da Hacker in jeder Zeitzone arbeiten können und Viren sich zu jeder Zeit verbreiten.

Alternativen und ihre Nachteile -
Statt arago Security-Lösung reine SOHO-Lösung (Blackbox)

- Kunden, die erkannt haben, dass eine durch den Provider bereit gestellte „shared Firewall“ nicht die erforderliche Sicherheit oder Performance bietet, entscheiden sich oft für eine eigene Firewall, die in der Regel auf SOHO-Komponenten/ Appliances basiert. Diese Lösungen werden dann in der Regel selbst administriert. Aufgrund ihrer Zielgruppe sind solche Systeme nicht wirklich für einen 24/7-Betrieb geeignet, dies bezieht sich sowohl auf die technische Haltbarkeit, als auch auf die Möglichkeiten zur Überwachung, zur sicheren Administration und zum Failover.

- Selbst wenn man hochpreisige Komponenten aus dem „Blackbox-Marktsegment“ verwendet, wird die Kombination in der Regel nicht das Leistungsspektrum von aMSO erreichen: aMSO verwendet Komponenten, die im Bankenbereich jahrelang erprobt und in großen Umgebungen eingesetzt werden.

- Derartige Lösungen haben immer einen großen Nachteil: Sicherheit veraltet sehr schnell. Schon nach einem halben Jahr ohne professionelle Betreuung hat eine Sicherheitsinfrastruktur den Großteil ihrer Wirkung verloren. Selbst wenn man im Unternehmen IT-Fachkräfte hat, die durch aufwändige Schulungen spezifisches Security-Wissen erworben haben, so wird in einem nicht auf Security spezialisierten Unternehmen solches Personal schon aus Kostengründen nicht rund um die Uhr verfügbar sein, um auf Angriffe zu reagieren, Sicherheitspatches einzuspielen oder ähnliche wichtige Aufgaben zu erledigen. Zudem sind diese Mitarbeiter oft überfordert, wenn es wirklich zu einem erfolgreichen Hackerangriff kommt, da die Erfahrung fehlt.

- arago schließt diese Lücke: aMSO bietet nicht nur die erprobte Sicherheitsinfrastruktur, arago bietet auch den gesicherten Betrieb 24 Stunden, 7 Tage die Woche. Und wenn es wirklich zu einer Sicherheitsverletzung kommt, helfen Ihnen unsere erfahrenen Administratoren mit genau dem Wissen, das sie sonst den Großbanken zur Verfügung stellen.

Alternativen und ihre Nachteile - DSL-Router mit „Firewall, Intrusion Detection ...“

- In Zeiten immer billiger werdender Breitbandverbindungen wird der Markt überschwemmt mit DSL- oder Standleitungsangeboten, oft mit eigenem Router. Fast jeder Hersteller solcher kleinen Internetrouter schmückt diese heute mit wohlklingenden Worten wie „Firewall“, „Intrusion Detection“ und „Virenschutz inklusive“.

- Als Kunde solcher Lösungen muss man sich bewusst sein, dass sich hinter diesen Ausdrücken fast nie das verbirgt, was man im professionellen Bereich darunter versteht.

- Die Firewalls sind oft einfache NAT-Router, Intrusion Detection beschränkt sich in der Regel auf einige wenige Angriffe, die man erkennen kann und der integrierte Virenschutz ist oft eine gebundelte CD mit einer Desktop-Virenschutzsoftware.

- Diese Lösungen können keinen ernsthaften Schutz bieten. Für einen gelegentlichen Internetbesuch mit einem privaten PC mögen sie geeignet sein – im Unternehmensbereich kosten die durch solche Systeme verursachten Probleme schon nach wenigen Monaten ein Vielfaches einer sinnvollen Lösung.

Alternativen und ihre Nachteile - Virenschutz auf dem Desktop oder dem Mailserver

- Oft wird, gerade bei kleineren Unternehmen, zwar eine Firewall implementiert, auf einen zentralen Virenschutz auf dem Gateway (Firewall) für Mail und Web jedoch verzichtet. Hier wird argumentiert, dass man ja bereits eine Virensoftware auf den (Desktop-)PCs verwendet.

- Dieser Schutz ist jedoch, wie die oben gezeigten Beispiele zeigen, trügerisch. Viren können ein ganzes Netz infizieren, schon bevor ein Desktop-Scanner sie erkennen kann. Zudem haben Desktop-Virenscanner den Nachteil, dass sie durch den Benutzer deaktiviert werden können und auch das Update der Pattern oft dem Benutzer überlassen wird. Die Funktionalität ist somit nicht garantiert.

- Zudem kann ein Virus oder ein Trojaner beim Öffnen einer Mail oder einer Webseite bereits aktiviert werden – bevor die Datei auf die Platte geschrieben wird und durch einen Datei-Virenscanner geprüft werden kann.

arago
Institut für komplexes Datenmanagement AG

Am Niddatal 3
60488 Frankfurt am Main

Tel.: +49 (0) 69/40 56 8-0
Fax: +49 (0) 69/40 56 8-1 11

www.arago.de
info@arago.de