Datenschutz *konkret*

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 1/2017

Liebe Leserin, lieber Leser,

die Vorbereitungen auf die EU-Datenschutz-Grundverordnung laufen und das Thema IT-Sicherheit drängt sich immer mehr in den Vordergrund. Apropos IT-Sicherheit. Wie ist es eigentlich um die Informationssicherheit in der Sozialwirtschaft gestellt? Mit dieser Frage haben wir unter der Federführung von Herrn Prof. Dr. Merz von der Hochschule Hannover, die Web-Server der 193 größten freigemeinnützigen Sozialunternehmen in Deutschland einer Prüfung unterzogen. Die spannenden Ergebnisse stellen wir auf Seite 8 vor.

Sie setzen Software von US-amerikanischen Unternehmen ein? Werden dabei bewusst oder unbewusst Daten in die USA übermittelt? 2016 wurde nach langen Verhandlungen das bisherige Safe-Harbor-Abkommen zwischen der EU und den USA durch das EU-US Privacy Shield ersetzt. Worauf Sie achten sollten, erfahren Sie auf Seite 5.

Wir wünschen eine aufschlussreiche Lektüre.

Thomas Althammer & Niels Kill

Datenschutz auch bei Pokémon Go!

Die mobile App Pokémon Go hat für viele Menschen einen regelrechten Suchtfaktor. Und das keineswegs nur für Jugendliche – auch viele Erwachsene sind dem Spiel geradezu verfallen.

Dabei darf der Datenschutz freilich ebenso wenig aus dem Blick geraten wie der Schutz von Unternehmensgeheimnissen. Noch im Februar kommt übrigens ein von den Fans sehnsüchtig erwartetes Mega-Update. Allzu schnell kann es besonderen Leichtsinn auslösen. In seiner Freizeit kann natürlich jeder tun, was er will – beispielsweise so viele Spiele-Monster erfolgreich jagen, dass er das nächste Level von Pokémon erreicht. Aber

In dieser Ausgabe:

was ist, wenn gerade auf dem Grundstück des eigenen Arbeitgebers wunderschöne Pokéstops zu finden sind? Wenn man also gerade dort die besten Monster einfangen kann?

Pokéstops, Arenen und Monster

Die Spielkundigen verstehen sofort, was mit diesen Dingen gemeint ist. Sie ziehen sich in eine Arena zurück, um ein paar Monster zu besiegen. Ihre Kollegen wiederum wundern sich, wie ganz normale Menschen der Faszination von Dingen erliegen, die für die anderen um sie herum gar nicht sichtbar sind.

Arbeitszeit ist keine Spielzeit!

Klar ist, dass Spielen während der Arbeitszeit schon deshalb Fragen aufwirft, weil dann gerade nicht gearbeitet wird. Das ist zwar kein Thema des Datenschutzes, sondern des Arbeitsrechts. Freilich: Mehr Schaden als eine Zigarettenpause, die zu Unrecht nicht als Arbeitspause registriert wird, richtet das kurze Einfangen eines virtuellen Monsters während der Arbeitszeit auch nicht an, oder?

Bilder von Monstern und anderen Dingen

Das kommt darauf an. Vielfach ist es üblich, eben eingefangene Monster zu fotografieren und das Foto an Freunde zu schicken. Blöd nur, wenn da noch andere Dinge auf dem Bild sind, etwa Konstruktionen, die nicht fotografiert werden dürfen. Wer weiß, wo ein solches Foto landet, und wer weiß, ob jeden Empfänger des Fotos wirklich nur die Monster interessieren.

Harmlose und andere Apps

Vielfach untersagen Unternehmen aus gutem Grund, Apps für private Zwecke auf dienstlichen Smartphones oder Tablets zu installieren. Ein solches Verbot gilt dann auch für die Pokémon-App. Das Argument, sie sei harmlos und könne keinen Schaden anrichten, kann daran nichts ändern. Erstens kommt es auf diesen Gesichtspunkt nicht an. Zweitens stellt sich die Frage, ob er zutrifft. Schon ein kurzer Blick in die Nutzungsbedingungen der App zeigt, dass sich der App-Anbieter das Recht einräumen lässt, unter bestimmten Bedingungen Daten an Dritte weiterzugeben. Was daraus im Einzelfall entstehen könnte, vermag niemand sicher abzuschätzen.

Selbstverständliche Spielregeln

Ein völliges No-Go ist es vor diesem Hintergrund, berufliche Mail-Adressen bei dem Spiel zu benutzen. Wer spielen will, sollte das bitte nur auf seinem privaten Gerät tun und dabei nur eine private Mail-Adresse verwenden. Und die rechte Zeit für das Spiel ist die Freizeit, nicht die Arbeitszeit. Wer diese Punkte beachtet, kann sein Spiel genießen und sich beim Monster-Kampf bestens erholen. &

Impressum

Redaktion/V. i. S. d. P.:
Niels Kill, Thomas Althammer

Haftung und Nachdruck:
Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Jeglicher Nachdruck, auch auszugsweise, ist nur mit vorheriger Genehmigung der Althammer & Kill GmbH & Co. KG gestattet.

Anschrift:
Althammer & Kill GmbH & Co. KG
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0 · Fax -48

Schutzgebühr Print-Ausgabe: 10,– €

Was bedeutet eigentlich „Stand der Technik“?

Der Datenschutz verlangt technisch-organisatorische Schutzmaßnahmen nach dem Stand der Technik. Das klingt nicht sehr konkret – mit Absicht!

Fast jeder zweite Internetnutzer (47 Prozent) ist in Deutschland in den vergangenen zwölf Monaten Opfer von Internetkriminalität geworden, so eine repräsentative Umfrage des Digitalverbands Bitkom. Die Vorfälle reichen von gefährlichen Infektionen durch Schadsoftware bis hin zu Online-Betrug und Erpressung.

Um die eigenen Daten zu schützen, aber auch um die Daten der Kunden, Partner und Mitarbeiter im Unternehmen zu schützen, sind also umfangreiche Maßnahmen für die Datensicherheit erforderlich.

Am schönsten wäre eine genaue Anleitung …

Doch welche Maßnahmen sind genau notwendig? Wie schützt man sich am besten? Der Bitkom-Verband schreibt dazu: Gegen digitale Angriffe nutzen vier von fünf Internetnutzern (80 Prozent) ein Virenschutz-Programm und zwei von drei (67 Prozent) eine Firewall auf ihrem Computer.

Antiviren-Programme und Firewall sind der absolute Basisschutz für jeden Computer. Aber reicht das aus? Was fordern zum Beispiel die Datenschutzvorschriften? Gibt es hier eine konkrete Vorgabe zum Schutzumfang?

BDSG und DSGVO nennen kaum genaue Sicherheitsverfahren

Im Bundesdatenschutzgesetz (BDSG) findet man: Eine Maßnahme für die Zugangskontrolle, Zugriffskontrolle und Weitergabekontrolle ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Die ab Mai 2018 anzuwendende Datenschutz-Grundverordnung (DSGVO) nennt die Verschlüsselung sowie die Pseudonymisierung.

Grundsätzlich aber sagen beide Gesetze zu den Maßnahmen der Datensicherheit: Geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, sind zu treffen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Statt Schutzverfahren aufzulisten, verweisen die Texte jeweils in erster Linie auf den Stand der Technik. Warum eigentlich?

IT und Bedrohungen dynamischer als Gesetzgebung

Die gesetzlichen Regelungen fordern Schutzmaßnahmen nach dem Stand der Technik, weil die IT-Sicherheitslösungen jeweils zur aktuellen Bedrohungslage, zum Schutzbedarf der Daten und zur eingesetzten IT passen müssen. Veraltete IT-Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz.

So sind zum Beispiel Verschlüsselungsverfahren, die vor einigen Jahren noch als Standard galten, heute kein wirksamer Schutz mehr. Datendiebe können diese Verschlüsselungsverfahren inzwischen relativ leicht brechen und umgehen.

Damit die Datensicherheit aktuell und damit hoch genug ist, müssen die Maßnahmen also regelmäßig angepasst und verstärkt werden. Würden rechtliche Vorgaben genaue IT-Sicherheitsverfahren benennen, müsste der Gesetzgeber die Texte fortlaufend ändern. Das geht natürlich nicht. Deshalb verlangen die Regelungen, dass die Datensicherheitsmaßnahmen aktuell sind und damit die Sicherheit den Stand der Technik abbildet.

Privat und beruflich am Puls der IT-Sicherheit bleiben

Für Sie als Anwender bedeutet dies, dass Sie jeweils aktuelle Lösungen für Ihre Datensicherheit benötigen. Am Arbeitsplatz sollten Sie sich an die IT-Sicherheitsrichtlinien der Firma halten und nur die entsprechend freigegebenen IT-Lösungen sowie Sicherheitsanwendungen nutzen.

Privat sind Sie erst einmal auf sich gestellt. Hier ist es aber ebenso wichtig, dass Sie auf eine aktuelle Datensicherheit achten. Nicht nur, wenn Sie Privatgeräte beruflich verwenden, sondern generell.

So könne eine Person etwa an ihrer Körperhaltung zu erkennen sein, aber auch an ihrer Kleidung oder an mitgeführten Gegenständen. Auch der Zeitpunkt und der Ort einer Aufnahme könnten Rückschlüsse darauf erlauben, welche Person man vor sich habe.

Was konkret tun?

Ihr aktuelles Datensicherheitsprogramm umfasst dabei, dass Sie die Betriebssysteme und Anwendungen auf allen genutzten Endgeräten aktuell halten und die Datenschutz- und Sicherheitsoptionen regelmäßig auf den passenden Stand bringen. Sicherheitslösungen wie den Virenschutz müssen Sie ebenfalls mit Updates versorgen. Zudem ist wichtig, dass Sie sich neue Versionen der Sicherheitsprogramme beschaffen, in der Regel einmal jährlich. Die täglichen Updates gelten nämlich in aller Regel der aktuellen Viren-Erkennung. Neue Sicherheitsfunktionen bekommen Sie meist erst mit einer neuen Version der Anwendung.

Ob sich der Umstieg auf andere Sicherheitslösungen lohnt oder nicht, sollten Sie abhängig machen von Testergebnissen renommierter Prüfinstitute und von Berichten in der Fachpresse. Sicher werden Sie auch in Schulungen und Unterweisungen zu IT-Sicherheit und Datenschutz jeweils aktuell informiert. Wichtig ist: Bleiben Sie am Ball. Die Datendiebe haben immer neue Ideen, wie sie angreifen können. &

Heartbleed feiert 3. Geburtstag – nach Jahren sind noch immer tausende Server angreifbar

Heartbleed nutzte eine Sicherheitslücke in OpenSSL-Bibliotheken aus, die seit 2011 herausgegeben wurden. Der Fehler ermöglichte Angriffe auf verschlüsselte Internetverbindungen, was insbesondere die Übermittlung von Zugangsdaten und diversen anderen sensiblen Daten anfällig machte.

Trotz der massiven Pressemeldungen aus dem Jahre 2014, ist Heartbleed anscheinend nicht totzukriegen.

Heartbleed im Jahr 2017

Der aktuelle Shodan-Report (https://www.shodan.io/report/DCPO7BkV) zeigt, dass noch immer mehr als 200.000 aus dem Internet erreichbare Systeme für die Heartbleed-Sicherheitslücke anfällig sind.

Wer im Jahr 2017 immer noch Systeme betreibt die für die OpenSSL-Lücke anfällig sind, muss davon ausgehen, dass diese Systeme bereits kompromittiert wurden.

Woran es genau liegt, dass noch so viele Systeme betroffen sind, ist nicht genau geklärt. Es dürfte aber schlicht eine ganze Reihe von Systemen geben, um die sich seit 3 Jahren niemand gekümmert hat. Wahrscheinlich auch deshalb, weil die Systeme ihre eigentliche Aufgabe seitdem schlicht erfüllen. &

Was ist der Privacy Shield?

Wer in einem Unternehmen arbeitet, das Daten in die USA übermittelt, muss ihn kennen. Aber auch jeder Normalbürger sollte zumindest einmal davon gehört haben. Die Rede ist vom Privacy Shield, auf Deutsch etwa „Schutzschild für das Persönlichkeitsrecht". Er kann seit dem 1. August 2016 genutzt werden. Viele Unternehmen hatten dringend darauf gewartet.

Will ein Unternehmen Daten von Kunden oder auch Daten von Mitarbeitern an ein US-Unternehmen übermitteln, geht das nicht „leicht und locker". Und zwar auch dann nicht, wenn es sich bei dem US-Unternehmen beispielsweise um die „US-Mutter" handelt.

Bekanntlich gehören die USA nicht zur EU. Deshalb erlauben die EU-Regelungen zum Datenschutz den Transfer von Daten in die USA nur dann, wenn dort ein angemessenes Datenschutzniveau herrscht. Was als angemessen anzusehen ist, bestimmt sich dabei natürlich nach den Vorstellungen der EU.

Datenschutz in den USA: durchaus, aber...

Damit beginnen in der Praxis die Probleme. Zwar gibt es in den USA sehr wohl Datenschutzvorschriften. Deshalb sollte man gegenüber Kollegen aus den USA auch nie zu überheblich davon sprechen, die USA würden sowieso keinen Datenschutz kennen.

Nur zu schnell kann es einem sonst passieren, dass diese Kollegen etwa auf Regelungen hinweisen, die die Daten von Kindern ganz besonders schützen. Die Abkürzung hierfür heißt COPPA (Children's Online Privacy Protection Rule) und ist auch den meisten Durchschnitts-Amerikanern bekannt.

Individuelle Einwilligungen: nur theoretisch denkbar

Die US-Regelungen setzen die Schwerpunkte aber ganz anders als die Vorschriften der EU. Manche Aspekte des Datenschutzes, die in Europa ganz hoch gehalten werden, gelten in den USA kaum etwas. Langer Rede kurzer Sinn: Ein Datenschutzniveau, das nach den Vorstellungen der EU generell als angemessen anzusehen wäre, existiert in den USA nicht.

Wie soll ein Unternehmen damit umgehen? Nun, es könnte beispielsweise jeden einzelnen Betroffenen um seine Einwilligung bitten und seine Daten erst dann übermitteln. Theoretisch wäre das denkbar. In der Praxis funktioniert das aber schon wegen des Aufwands nicht. Deshalb wählt der neue Privacy Shield einen anderen Ansatz.

Der besondere Ansatz von Privacy Shield:

- Ein US-Unternehmen, das personenbezogene Daten aus der EU erhalten soll, verpflichtet sich dazu, umfangreiche Spielregeln für den Datenschutz einzuhalten. Sie sind unter dem Begriff „Privacy Shield" zusammengefasst.
- Diese Verpflichtung erfolgt gegenüber den zuständigen US-Behörden. Das ist meist die Federal Trade Commission (FTC), eine Verbraucherschutzbehörde.

– Der Inhalt der Spielregeln ist zwischen dem US-Handelsministerium (Department of Commerce) und der Europäischen Kommission abgestimmt.
– Ist ein US-Unternehmen eine solche Verpflichtung eingegangen, gilt das Datenschutzniveau in diesem Unternehmen auch seitens der EU als angemessen.
– Die positive Folge für die europäischen Geschäftspartner solcher US-Unternehmen: Sie dürfen personenbezogene Daten an dieses Unternehmen unter denselben Voraussetzungen übermitteln, unter denen dies auch innerhalb der Europäischen Union zulässig wäre.

Keine Einwilligung der Betroffenen nötig

Die Betroffenen müssen nicht gefragt werden, ob sie damit einverstanden sind. Sie müssen aber in geeigneter Weise informiert werden. Dabei sind viele Einzelheiten zu beachten, um die sich die Spezialisten in den Unternehmen kümmern. In Deutschland sind dies die Datenschutzbeauftragten der Unternehmen.

Erinnern Sie sich noch an Safe Harbor?

Manchem wird dieses Vorgehen irgendwie bekannt vorkommen. Völlig zu Recht! Ziemlich ähnlich lief dies auch schon bei den Safe-Harbor-Regelungen ab. Sie hatten sich über zehn Jahre lang beim Transfer von Daten aus der EU in die USA bewährt – jedenfalls aus der Sicht der meisten Unternehmen.

Allerdings hatte der Europäische Gerichtshof diese Regelungen im Oktober 2015 aus verschiedenen Gründen gekippt. Das geschah gewissermaßen über Nacht, also ohne jede Übergangsfrist. Deshalb waren neue Regelungen, wie sie der Privacy Shield nun vorsieht, dringend erforderlich. Etwas vereinfacht lässt sich sagen: Der Inhalt des Privacy Shield ist neu und wesentlich ausgefeilter, als es die Regelungen von Safe Harbor waren. Der Verfahrensablauf ist aber ziemlich ähnlich.

Gegen die Spielregeln verstoßen? Lieber nicht!

Wie sieht es übrigens damit aus, dass sich die Unternehmen auch wirklich an die Spielregeln halten, zu denen sie sich verpflichtet haben? Die Chancen dafür stehen gut. Jeder weiß, wie kräftig US-Behörden bei Rechtsverstößen zupacken können. Und das gilt nicht nur, wenn es um Verstöße gegen Abgasregelungen geht. Auch Datenschutzverstöße von US-Unternehmen haben die amerikanischen Behörden schon schwer geahndet. Gehen Sie also davon aus: Privacy Shield ist ernst gemeint! &

Virenschutz oder Datenschutz?

Die Frage, ob Sie Virenschutz oder Datenschutz wollen, erscheint auf den ersten Blick absurd. Denn Sie brauchen beides. Tatsächlich aber können Virenschutz-Lösungen zum Problem für den Datenschutz werden.

Kaum jemand verzichtet komplett auf einen Virenschutz für den PC oder das Notebook, eigentlich sollte es niemand tun. Bei Smartphones sieht es schon deutlich schlechter aus: Jeder fünfte Smartphone-Besitzer (20,7 %) nutzt sein Mobilgerät ohne jegliche Sicherheitsfunktionen zum Schutz des Geräts und der darauf befindlichen Daten, so eine Umfrage für das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Aus Sicht des Datenschutzes sollte auf jedem Endgerät ein Schutz vor Malware oder Schadsoftware vorhanden sein. Doch diese Forderung kann zu einem Datenrisiko führen, wenn man nicht darauf achtet, wie es der Anbieter der Antiviren-Software mit dem Datenschutz hält.

Tatsächlich gibt es eine ganze Reihe von Virenschutz-Lösungen, die zwar Malware erkennen und abwehren, die es aber selbst nicht so genau mit dem Datenschutz zu nehmen scheinen.

Überprüfung von Datenschutzerklärungen ergab Mängel

Das Testinstitut AV-Test aus Magdeburg hat die Datenschutzerklärungen von 26 Antiviren-Programmen untersucht und dabei viele Unzulänglichkeiten und Probleme entdeckt.

So hatten zwei Anti-Malware-Lösungen überhaupt keine Datenschutzerklärung. In fast jeder untersuchten Datenschutzerklärung räumten sich die Hersteller zudem in erheblichem Umfang Zugriffsrechte auf Daten ein, die für den Einsatz einer Schutz-Software nicht nötig sein dürften, so AV-Test.

Einige Extrembeispiele untermauern diese Einschätzung: So haben einzelne Hersteller angegeben, dass sie Daten über das Geschlecht, die Berufsbezeichnung sowie Rasse und sexuelle Orientierung eines Nutzers verarbeiten wollen. Der Bezug zum Schutzzweck der Software ist offensichtlich nicht vorhanden. Die Vermutung liegt nahe, dass die Anbieter Nutzerinformationen zu Werbezwecken erheben bzw. an Dritte für Werbemaßnahmen weitergeben. Eine informierte Einwilligung, wie sie der Datenschutz fordert, erfragen sie dafür vom Nutzer nicht.

Leider können Sie also nicht davon ausgehen, dass alle Lösungen, die Ihre Daten vor Angreifern schützen, selbst mit den Daten so umgehen, wie es der Datenschutz verlangt. Auch IT-Sicherheitsanwendungen müssen hinterfragt werden, wie sie es mit dem Datenschutz halten, genau wie jede andere Applikation, die Sie installieren oder nutzen möchten.

Kein blindes Vertrauen in die IT-Sicherheit

Genau genommen sollten Sie bei IT-Sicherheitslösungen wie den Antiviren-Programmen noch genauer hinschauen, was in der Datenschutzerklärung steht. Denn Sicherheitsprogramme haben sehr mächtige Funktionen und oftmals weitgehende Zugriffsberechtigungen auf die Daten. Diese Berechtigungen brauchen sie in Teilen zwar, um wirklich schützen zu können. Doch sie machen auch einen falschen Umgang mit personenbezogenen Daten durch Sicherheitssoftware so gefährlich.

Nutzen Sie also auf jedem Endgerät einen Virenschutz, aber prüfen Sie bei jedem Tool auch die Datenschutzerklärung. Virenschutz und Datenschutz werden beide gebraucht, getrennt voneinander sollten sie nicht sein. Ohne Virenschutz ist Datenschutz heute nicht mehr möglich, ohne Datenschutz sollte es jedoch keine Virenschutz-Lösung geben. &

Virenschutz = Datenschutz? Testen Sie Ihr Wissen!

Frage: Virenschutz ist elementar für den Datenschutz. Stimmt das?

a. Ja, das stimmt. Trotzdem ist der Datenschutz beim Virenschutz nicht automatisch garantiert.
b. Virenschutz braucht man nur, wenn man das Internet nutzt.
c. Virenschutz-Lösungen berücksichtigen automatisch den Datenschutz.

Lösung: Die Antwort a. ist richtig. Virenschutz braucht man auf jedem Endgerät, gleich ob es einen Internetzugang hat oder nicht. Denn auch ein USB-Speicherstift kann zum Beispiel Malware einschleppen. Trotzdem kann man nicht davon ausgehen, dass der Datenschutz beim Virenschutz automatisch stimmt. Prüfen Sie die Datenschutzerklärung des Anbieters genau, bevor Sie sich für eine Lösung entscheiden.

Frage: Antiviren-Software verarbeitet personenbezogene Daten nur zu Sicherheitszwecken. Stimmen Sie dem zu?

a. Ja, zu welchen Zwecken sollte ein Sicherheitsprogramm denn sonst Daten verarbeiten?
b. Man sollte in der Datenschutzerklärung prüfen, zu welchen Zwecken der Software-Anbieter personenbezogene Daten erhebt, nutzt und speichert. Man kann Erstaunliches finden …

Lösung: Die Antwort b. ist richtig, wie eine Untersuchung von AV-Test ergeben hat. Ob die erhobenen Nutzerdaten wirklich dem Sicherheitszweck dienen oder nicht, können Sie sich klarmachen, indem Sie die Sicherheitsfunktionen betrachten und sich fragen, ob Sie diese denn möchten oder nicht. So kann ein Zugriff auf die Standortdaten sinnvoll sein, wenn Sie die Funktion nutzen wollen, ein verlorenes oder gestohlenes Gerät wiederzufinden. Daten über das Geschlecht und die sexuelle Orientierung des Nutzers haben aber zweifellos nichts mit den Sicherheitsfunktionen zu tun. Trotzdem wollen manche Antiviren-Lösungen solche Daten erheben und verarbeiten. Hier ist mehr als Vorsicht angesagt – es empfiehlt sich die Suche nach einer anderen Antiviren-Software!

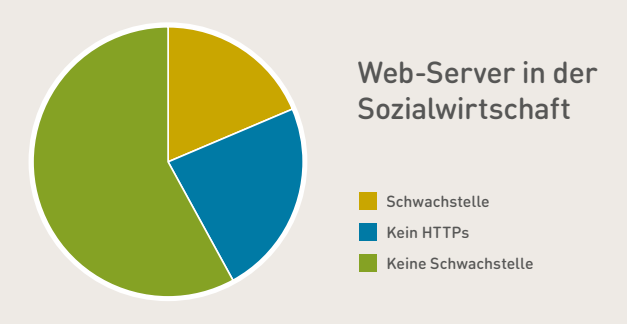
Studie zur Sicherheit von Web-Servern in der Sozialwirtschaft

Untersuchung von Web-Servern führender Sozialunternehmen auf Nutzung von Verschlüsselungsverfahren per https, Schwachstellen beim Einsatz von SSL/TLS und die Berücksichtigung gesetzlicher Vorgaben

Die Web-Präsenz eines Unternehmens ist Aushängeschild im Internet und längst für nahezu alle Unternehmen unverzichtbar. Deshalb sollte die Verfügbarkeit des Web-Servers und die Integrität der auf dem Server gespeicherten und zur Verfügung gestellten Daten jederzeit gewährleistet sein.

Bedeutung der Web-Sicherheit für Unternehmen

Bei Unternehmen, bei denen der Web-Server innerhalb des eigenen IT-Netzes betrieben wird, kann der Web-Server als eine für alle Internet-Teilnehmer sichtbare Eingangstür in das Unternehmensnetz angesehen werden. Dass diese Tür einen guten Schutzmechanismus benötigt, liegt auf der Hand. Ein potenzieller Angreifer wird zudem von der (Un-)Sicherheit des oder der Web-Server auf die (Un-)Sicherheit des gesamten IT-Netzes schließen: Wird beispielsweise die Software auf einem Web-Server nicht aktualisiert und Sicherheitslücken nicht behoben, so wird dies wahrscheinlich auch bei anderen IT-Komponenten der Fall sein. So gesehen, stellt die Sicherheit des Web-Servers einen Indikator für ein funktionierendes Sicherheitsmanagement im Unternehmen dar. Die durchgeführte Studie erlaubt also in Grenzen Rückschlüsse von der Web-Server-Sicherheit auf die Sicherheit des gesamten IT-Verbundes und damit auf das Vorhandensein eines funktionierenden IT-Sicherheitsmanagements.



SSL-Schwachstellen bei 188 Web-Servern aus dem Sozialwesen

Relevanz und rechtliche Grundlagen

Sozialunternehmen verarbeiten teils äußerst sensible personenbezogene Daten, für die ein hoher Schutzbedarf besteht. Werden solche Daten über die Web-Präsenz der Organisation ausgetauscht, müssen insbesondere Schutzmaßnahmen nach dem Stand der Technik getroffen werden,

```
HTTP/1.1 200 OK
Date: Thu, 17 Mar 2016 08:40:30 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.45-0+deb7u2
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
```

In diesem HTTP-Header sind die Versionsnummern des Apache-Web-Servers sowie der PHP-Engine (in Pink dargestellt) enthalten. Anhand der Versionsnummern lässt sich nun u. U. ermitteln, wie alt die eingesetzte Software ist und ob sie bekannte Schwachstellen enthält.

um die Integrität und Vertraulichkeit der übermittelten Daten sicherstellen.

Als anerkannter Stand der Technik bei der Nutzung von Angeboten im Internet gilt der Einsatz von Zertifikats-basierten Verschlüsselungsverfahren per SSL/TLS. Ein sicherer Zugriff schafft Vertrauen, der durch eine Client-seitige Überprüfung in den gängigen Web-Browser verifiziert und entsprechend gekennzeichnet wird.

Hersteller von Internet-Browsern haben angekündigt, in Zukunft vermehrt bei Besuch unverschlüsselter Websites zu warnen. Der Einsatz von SSL/TLS auf einer Website wirkt sich positiv auf das Ranking bei Suchmaschinen aus.

Untersuchte Organisationen

Insgesamt wurden 193 Organisationen aus dem Bereich des Sozialwesens betrachtet. Es handelt sich hierbei um die größten freigemeinnützigen Sozialunternehmen in Deutschland, jeweils bezogen auf die Regionen Nord, Ost, West und Süd. Grundlage war eine entsprechende Veröffentlichung der Zeitschrift Wohlfahrt Intern in der Ausgabe 09/2015.

Die untersuchten Organisationen gehören zu den Spitzenverbänden der Freien Wohlfahrtspflege von Arbeiterwohlfahrt (AWO), dem Deutschen Caritasverband (Caritas), dem Paritätischen Wohlfahrtsverband (der Paritätische), dem Deutschen Roten Kreuz (DRK) und der Diakonie Deutschland (Diakonie). Nach Angaben des veröffentlichten Rankings erwirtschaften sie insgesamt einen Umsatz von rund 28 Milliarden Euro.

Methoden zur Überprüfung der Sicherheit von Web-Servern

Für die Überprüfung von IT-Systemen über das Netzwerk bzw. das Internet gibt es viele verschiedene Werkzeuge. Ein häufig eingesetztes Werkzeug ist der Port-Scanner, der alle aus dem Internet erreichbaren Dienste bzw. Ports ausfindig macht. Für die einzelnen Dienste wie z.B. Web-Server, E-Mail-Server oder Netzwerkfreigabe gibt es spezielle Werkzeuge, die nach Schwachstellen suchen oder sie ausnutzen. Auch existieren umfangreiche, allgemeine Schwachstellen-Suchwerkzeuge (Vulnerabilty scanner) und Werkzeuge zum Ausnutzen (Exploit) von Schwachstellen.

Für Web-Server gibt es spezialisierte Tools, die Schwachstellen in der Konfiguration oder in der Software selbst finden, sowie Tools, die Schwachstellen in Content Management Systemen aufdecken. Viele der Werkzeuge sind frei verfügbar und stehen Angreifen wie IT-Sicherheitsprüfern (Penetrationstestern) gleichermaßen zur Verfügung.

In der Studie angewandte Methoden

IT-Sicherheitsüberprüfungen dürfen im Allgemeinen nur mit Erlaubnis des überprüften Unternehmens durchgeführt werden; z. B. dann, wenn Schwachstellen nicht nur aufgedeckt, sondern auch ausgenutzt werden. Selbst einfachere Überprüfungen wie Port-Scans sind u.U. nicht zulässig, da diese Überprüfungen die untersuchten Systeme und Netzwerke unter Last stellen.

Kennung	Name	Geschlossen seit:
CVE-2014-0160	OpenSSL „Heartbleed" Schwachstelle	April 2014
CVE-2014-0224	„CCS Injection" Schwachstelle	Juni 2014
CVE-2014-3566	SSLv3 Schwachstelle „Poodle"	Oktober 2014
CVE 2015-4000	DiffieHellman-Schwachstelle „logjam"	Mai 2015

Daher wurde hier von solchen Prüfungen abgesehen und nur einfache Prüfungen, die im Zuge eines einfachen Web-Seiten-Abruf erfolgen, durchgeführt. Ein Beispiel hierfür ist die Überprüfung der von Web-Servern übermittelten Versionsnummern der eingesetzten Software.

Da nicht alle Server diese Versionsnummern übertragen und man nicht immer auf mögliche Schwachstellen schließen kann, wurde eine weitere Überprüfung durchgeführt. Während des Verbindungsaufbaus mit einem Web-Server, der Verschlüsselung unterstützt, kann ermittelt werden, ob die verwendete Verschlüsselungssoftware (SSL) Schwachstellen enthält, ohne dass diese ausgenutzt oder der Server in einer anderen Form in seiner Funktion beeinträchtigt wird.

Mit Hilfe der Kennung können zu den einzelnen Schwachstellen ausführliche Informationen unter http://www.cvedetails.com abgerufen werden. Es handelt sich um Schwachstellen mit hohem Bekanntheitsgrad, die in 2014 bzw. 2015 geschlossen wurden. Als Werkzeug zur Überprüfung wurde nmap eingesetzt, welches in der Lage ist, gezielt und ausschließlich nach den vier Schwachstellen zu suchen ohne den Server zu beeinträchtigen.

Interpretation der Ergebnisse

Die Untersuchungsergebnisse zeigen: Ungefähr ein Viertel der untersuchten Organisationen erlauben keine verschlüsselten Verbindungen zu ihren Web-Servern. Von den Verbleibenden setzt ca. ein Viertel aller Organisationen veraltete Software mit Schwachstellen ein. Nur 58% der Organisationen scheinen ihre Web-Server-Software auf aktuellem Stand zu halten und Verschlüsselung für erforderlich zu halten.

SSL-Schwachstellen bei 188 Web-Servern aus dem Sozialwesen

Dies ist ein klares Indiz dafür, dass bei vielen Sozialunternehmen kein richtiges Sicherheitsmanagement existiert, welches die regelmäßige Aktualisierung und damit Schwachstellenbereinigung der Web-Server-Software vorsieht. Es lässt sich vermuten, dass dies auch für andere Organisations-IT gilt. Die Vorgaben des im Juli 2015 in Kraft getretenen IT-Sicherheitsgesetzes sind insofern vielfach nicht in der Praxis umgesetzt.

Aufgrund der Rahmenbedingungen wurde nur nach vier Schwachstellen gesucht. Es steht zu befürchten, dass eine weitaus umfangreichere Untersuchung einen deutlich höheren Anteil an verwundbaren Systemen aufdecken würde. Auch unterstützen nicht alle Unternehmen verschlüsselte Verbindungen, was aus Sicherheitsgründen der Fall sein sollte. Über diese Unternehmen liefert die Studie keine Zahlen bzgl. der Schwachstellen.

Handlungsempfehlung für Unternehmen

Die untersuchten Sozialunternehmen sollten dringend ihr Sicherheitsmanagement überprüfen und gegebenenfalls anpassen. Regelmäßiges Einspielen von Sicherheitsupdates bzw. Software-Upgrades bei allen IT-Systemen stellt eine vergleichsweise einfache Sicherheitsmaßnahme mit großer Wirkung bzw. hohem Nutzen dar. Es kann auch sinnvoll sein, das Sicherheitsniveau von einem externen Dienstleister überprüfen zu lassen. Ebenso existieren Werkzeuge, wie z. B. Open-VAS, um die eigenen IT-Systeme auf Schwachstellen zu prüfen.

Konkret sich nur auf die hier beschriebenen Schwachstellen zu konzentrieren ist weder sinnvoll noch ausreichend. Ein Konzept zur regelmäßigen oder automatischen Durchführung von Softwareupdates einschließlich Überprüfung auf Umsetzung ist der einzige verlässliche Weg, um Schwachstellen möglichst schnell nach ihrer Veröffentlichung zu schließen.

Zusammenfassung

Die Studie hat gezeigt, dass bei einer erheblichen Anzahl an Organisationen aus dem Sozialwesen Nachholbedarf bezüglich der Umsetzung IT-Sicherheitsmaßnahmen besteht. Der Einsatz von Verschlüsselung und regelmäßige Software-Updates im Rahmen des IT-Sicherheitsmanagements sind obligatorisch und verhindern, dass Schwachstellen, wie die hier untersuchten über das Internet ausgenutzt werden können.

Bei der Kommunikation mit Sozialunternehmen spielen Vertraulichkeit und Integrität eine besondere Rolle: Es kann jedem Betreiber von Websites nur empfohlen werden, https-geschützte Verbindungen anzubieten, diese regelmäßig auf Sicherheitslücken zu überprüfen und ein umfassendes IT-Sicherheitsmanagementsystem aufzubauen. &

Benötigen Sie weitere Informationen?

Die vollständige Studie stellen wir Ihnen auf Wunsch gerne kostenlos zur Verfügung. Einfach eine E-Mail schreiben an:

info@althammer-kill.de

Termine

Wir freuen uns auf persönliche Begegnungen –
zum Beispiel im Rahmen der folgenden Veranstaltungen:

21.–23.02.2017, Mühltal
Ausbildung IT-Sicherheitsbeauftragte
Fokus Kirche, Non-Profits und Sozialwirtschaft

07.03.2017, Online, stifter-helfen.de
Geschäftsführer Haftung
Vortrag mit Strafen und Bußgeldern zum Angst machen

09.–10.03.2017, Eichstätt
Fachtagung Sozialinformatik mit Workshop von Althammer & Kill
Das „Familientreffen" der Branche in Eichstätt

20.–24.03.2017, Hannover
CeBIT 2017
Besuchen Sie uns in Halle 5, Stand G27. Wir freuen uns auf Ihren Besuch!

28.03.2017, Hannover / 19.04.2017 Düsseldorf
EU Datenschutz-Grundverordnung
Wie sich Unternehmen vorbereiten sollten

25.–27.04.2017, Dortmund
Ausbildung Datenschutzbeauftragte
Fokus Kirche, Non-Profits und Sozialwirtschaft

Termin verpasst? Anruf oder E-Mail genügt und wir lassen Ihnen gern weitere Informationen zukommen.

News

Aus unserem aktuellen Newsletter:

Heartbleed feiert 3. Geburtstag
https://www.althammer-kill.de/news-detail/Heartbleed-feiert-3ten-geburtstag.html

Angeln auf Google-Passwörter
https://www.althammer-kill.de/news-detail/angeln-auf-google-passwoerter.html

Rückblick 2016 und Vorschau auf 2017
https://www.althammer-kill.de/news-detail/rueckblick-auf-2016-und-vorschau-auf-2017.html

Risiko für kommerzielle Website-Betreiber beim Setzen von Links
https://www.althammer-kill.de/news-detail/risiko-fuer-kommerzielle-website-betreiber-beim-setzen-von-links.html

Security beim IoT (Internet der Dinge)
https://www.althammer-kill.de/news-detail/security-beim-iot-internet-der-dinge.html

Achtung Datenschutz-Kontrolle!
https://www.althammer-kill.de/news-detail/achtung-datenschutz-kontrolle.html

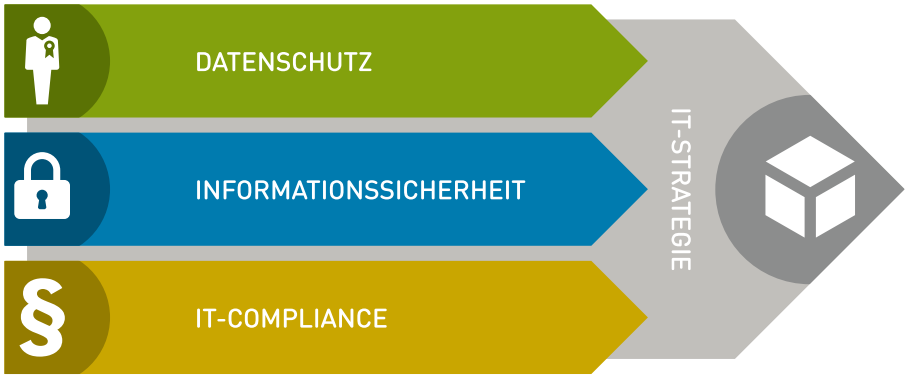
Anmeldemöglichkeiten zu unserem Newsletter finden Sie unter:
www.althammer-kill.de

12 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 1/2017

ALTHAMMER & KILL

Althammer & Kill – Wir schützen Ihre Daten.

Althammer & Kill ist ein auf Datenschutz, Informationssicherheit und IT-Compliance spezialisiertes Unternehmen. Unsere Mitarbeiter sind zertifizierte Datenschutzbeauftragte, IT-Sicherheitsexperten, ausgebildete IT-Compliance-Beauftragte und IT-Berater.



Datenschutz

Durch unsere langjährige Erfahrung in unterschiedlichsten Branchen können wir praxisgerechte Lösungen für Ihr Unternehmen entwickeln. Sei es im Rahmen eines konkreten Projektes oder als langfristige Begleitung Ihres Unternehmens z. B. in der Funktion als externer Datenschutzbeauftragter.

Informationssicherheit

Sind Ihre Systeme sicher? In unserer vernetzten Welt fällt es immer schwerer, den Durchblick zu behalten. Angriffe von außen oder ungewollter Informationsverlust: die Risiken sind vielfältig. Wir begleiten Sie zu Security-Fragen, prüfen die Sicherheit Ihrer Systeme und stellen den IT-Sicherheitsbeauftragten.

IT-Compliance

Gesetze, Verordnungen, Normen – da fällt es nicht immer leicht, Compliance-Verstöße zu verhindern. Wir begleiten branchenorientiert und liefern passende Konzepte für einen rechtssicheren Betrieb Ihres Unternehmens, z. B. im Rahmen des Risiko- und Notfallmanagements.

IT-Strategie

Welche Ziele möchten Sie mithilfe der Informationstechnologie in Ihrem Unternehmen erreichen? Wo liegen Möglichkeiten, Nutzen und Wertschöpfung? Wir orientieren unsere Arbeit an Ihren Zielen und begleiten bei der Auswahl und Gestaltung passender Strategien.

Wir sind Mitglied der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), des Berufsverbandes der Datenschutzbeauftragten Deutschlands e. V. (BvD) und des Fachverbands Informationstechnologien in Sozialwirtschaft und Sozialverwaltung e. V. (FINSOZ). &

Niels Kill
Geschäftsführer
Tel. +49 211 936748-20
nk@althammer-kill.de

Thomas Althammer
Geschäftsführer
Tel. +49 5139 973949-2
ta@althammer-kill.de

Frank Keusemann
Fachkraft für Arbeitssicherheit
Tel. +49 211 936748-60
fk@althammer-kill.de

Mariusz Bucki
Berater für IT-Sicherheit u. Datenschutz
Tel. +49 211 936748-30
mb@althammer-kill.de

Lars Begerow
Berater für IT-Strategie
Tel. +49 211 936748-40
lb@althammer-kill.de

Andreas Klostermann
Berater für IT-Sicherheit
Tel. +49 211 936748-0
ak@althammer-kill.de

Dr. Jan Holling
Berater für Datenschutz
Tel. +49 5139 973949-4
jh@althammer-kill.de

Andreas Hellmann
Berater für Datenschutz u. IT-Sicherheit
Tel. +49 211 936748-34
ah@althammer-kill.de

Katja Borchhardt
Organisation & Marketing
Tel. +49 211 936748-0
kb@althammer-kill.de

Althammer & Kill GmbH & Co. KG

info@althammer-kill.de
www.althammer-kill.de

Hauptsitz Düsseldorf:
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0 · Fax -48

Standort Hannover:
Buchenhain 15 · 30938 Burgwedel
Tel. +49 5139 973949-0 · Fax -9

Mitglied im:

FINSOZ e.V. · GDD Mitglied · BvD e.V. Mitglied · Hannover IT