

Sicher sind wir sicher

Wissen Sie, wie viele Türen Ihr
Netzwerk hat?

Es sind 65.536! Eine Zahl, die
überzeugt, wenn es um die
Frage geht, ob es sich lohnt,
in ein EDV-Sicherheitssystem
zu investieren.

Ein Bericht von Petra Otto,
DRK-Schwesternschaft
Hamburg e.V.



Die Würfel waren gefallen. Jeder Arbeitsplatz in der Schwesternschaft sollte einen Internetzugang erhalten und wir wollten uns vernetzen - mit unserem Bildungszentrum und unserer Senioreneinrichtung in Pinneberg. Zudem war es an der Zeit, für unsere Führungskräfte die Möglichkeit zu schaffen, sich von unterwegs oder auch von zu Hause mit dem eigenen Laptop auf den Server der Schwesternschaft einzuloggen. Auch für mich in meinen Bereich Öffentlichkeitsarbeit sollte es möglich sein, vom Home-Office aus zu agieren und jederzeit auf relevante Daten zugreifen zu können.

Beratung durch Profis

Wie kann das gelingen, ohne sensible Daten der Ausspähung preiszugeben und ohne Viren einzufangen? Nicht auszudenken, wenn der zentrale Server durch eine Unachtsamkeit, eine harmlos wirkende Mail oder eine arglos angesurft Website sabotiert würde. Und wer sollte unter diesen Umständen die Pflichten eines Datenschutzbeauftragten wahrnehmen, der laut §4 des Bundesdatenschutzgesetzes (BDSG) für alle Unternehmen - auch Vereine - vorgeschrieben ist, sofern mit personenbezogenen Daten gearbeitet wird und mehr als vier Mitarbeiter beschäftigt sind? Recht schnell wurde der

Entschluss gefasst, professionellen Rat einzuholen. Die Aufgabe war eine neue Infrastruktur und rechtliche Absicherung. Wir zogen eine Fachfirma hinzu und ließen uns beraten, wie der nächste Schritt ins sicher vernetzte Informationszeitalter aussehen müsste. Zunächst einmal sollte eine Risikoanalyse Aufschluss darüber geben, welche Sicherheitslücken unserer EDV Angreifern als Einladung dienen. Ob es überhaupt solche Schwachpunkte gibt, war gar nicht die Frage. „Jeder Rechner, der mit dem Internet verbunden ist, wird stündlich mehrere Male Zielscheibe von Angreifern, die versuchen, sich als Administrator anzumelden und ihr Unwesen zu treiben. Das ist bei Ihnen nicht anders“, erklärten uns die Fachleute. Gelingt dies, so ist dem Missbrauch Tür und Tor geöffnet. Daten sind in Gefahr, gestohlen, verfälscht und zweckentfremdet zu werden. Anwendungen wie beispielsweise Word, Excel oder das Abrechnungssystem unserer Senioreneinrichtung könnten lahm gelegt werden. Wer sich nun vorstellt, dass auf der gegnerischen Seite pubertierende jugendliche Hacker sitzen und Passwort um Passwort ausprobieren, liegt völlig falsch. Die Angriffe erfolgen vollautomatisch. Programme vollführen die Spionageakte. Tagelang, nächtelang, wochenlang. Das kostet die Angreifer nichts und irgendwann ist schon rein statistisch fette

Beute zu machen. Auf der Strecke bleiben dabei all die Opfer, bei denen „vermeintlich“ nichts zu holen ist. Keinesfalls wollten wir uns opfern!

Vertrauliche Daten

Schließlich geht es nicht um anonyme Datenbestände, sondern um die vertraulichen Daten unserer Mitglieder oder Fortbildungsteilnehmer. Umsicht auf allen Ebenen der Zusammenarbeit ist geboten. Also musste eine Lösung her, die uns zu vernünftigen Kosten einen modernen und zukunftssicheren Security-Standard verschafft. Eine sichere Vernetzung über Internetverbindungen zu unseren Betriebsbereichen und zu unseren Heimarbeitsplätzen - das war die Aufgabe, die wir der von uns gewählten Firma stellten. Auch die Verantwortung, dass alle Sicherheitseinrichtungen ordnungsgemäß arbeiten und alle rechtlichen Auflagen eingehalten werden, delegierten wir an den Dienstleister.

Firewall als Schaltzentrale

Professionell wurden unsere Anforderungen umgesetzt. Unser Netzwerk und unsere Internetverbindungen wurden, wenn wir das Ganze mit einem Auto vergleichen, mit ABS und Alarmanlage ausgestattet. Korrekt betitelt

Ein Alptraum: Was passiert, wenn der zentrale Server abstürzt? Alle Einrichtungen wären komplett lahm gelegt.

hört unsere neue Sicherheitsschaltzentrale auf den Namen „Firewall mit integriertem IPS“ (Intrusion Protection System). Sie passt auf, dass niemand unseren Server anzapft, der dazu nicht berechtigt ist. Sie schickt auch infizierte E-Mails in Quarantäne, so dass Viren uns erst gar nicht erreichen. Und eines kann die Firewall besonders gut: normale Internetverbindungen so abschotten, dass wirklich niemand (keine Software und kein Mensch) sie ausspähen kann. Zu diesem Zweck wird ein virtueller Tunnel im Internet aufgebaut, den wir genau in dem Moment exklusiv nutzen können, wenn wir ihn benötigen. Virtual Private Network (VPN) heißt diese geniale „Käseglocke“, in deren Schutz wir nun Personal- und Abrechnungsdaten von unseren externen Einrichtungen zum zentralen Server in die Verwaltung schicken. Und dies mit dem guten Gefühl, dass niemand, außer der vorgesehene Empfänger, sie zu Gesicht bekommt! Für die Zukunft planen wir sogar, über dieses VPN ein internes, sicheres Diskussionsforum für unsere Mitgliedsschwestern einzurichten.

Den Leistungsumfang, den wir als Schwesternschaft mit ausgegliederten Einrichtungen und mobilen Benutzern benötigten, hätten private Firewalls übrigens nie erfüllen können. Die Bedrohungssituation ändert sich ständig, so dass die Firewall ein differenziertes Regelwerk unterstützen muss. Auch die gesamte Sicherheitseinrichtung zentral von extern aus managen zu lassen, wäre mit einer privaten Firewall nicht möglich. Heute bekommen wir stattdessen monatliche Protokolle und Auswertungen der Firewall zugesandt, ohne dass wir uns um deren Pflege und Wartung kümmern müssen.

Zugunsten sicherer Kommunikationswege und auch aus Kostengründen stiegen wir auf eine neue Kommunikationssoftware um. Die Bedenken unserer Mitarbeiterinnen, die eine lange Umstellungsphase erwarteten, konnten schnell zerstreut werden. Die Umstellung auf das neue Programm war einfach und niemand

von uns möchte es jetzt mehr missen. Egal ob wir heute E-Mails, Faxe oder interne Nachrichten austauschen oder mobil auf unseren gemeinsamen Seminarkalender zugreifen. Das Programm legt alle digitalen Informationen direkt auf unserem zentralen Server übersichtlich ab.

Anfangs waren wir skeptisch, was die so genannten Benutzerrechte anging. Zu Unrecht, wie sich in der Praxis schnell herausstellte. Die Software sperrt Informationen tatsächlich zuverlässig für Personen, die nicht autorisiert sind, diese einzusehen. Im Extremfall könnten wir für jedes Dokument definieren, wer es sehen darf und wer nicht.

Risiken bewusst machen

Im Zuge der Umstellung hatten wir eine wichtige Lektion zu lernen. Nämlich dass wir selbst ein Risikofaktor für unsere IT-Sicherheit sind und dass unser Verhalten im Zweifel jegliche Technologie aushebeln kann.

Eine goldene Regel besagt beispielsweise, dass NIEMALS am Telefon ein Passwort weitergegeben wird. Klingt selbstverständlich - aber was tun Sie, wenn ein vermeintlicher „technischer Supporter“ anruft und ihr Passwort abfordert, damit er einen ins Stocken geratenen Prozess wieder in Gang setzen kann? Hand aufs Herz: Schöpfen Sie Verdacht, dass es sich um „Social Hacking“ handelt oder helfen Sie dem freundli-



chen Kollegen mit Ihren Zugangsdaten weiter? Ein anderes Beispiel: Viren und Würmer haben über Ihre offiziellen Internetverbindungen keine Chance, in Ihr Netzwerk einzudringen. Ganz anders sieht das aus, wenn Sie mal eben Ihre privaten E-Mails über web.de oder yahoo.de checken oder wenn Sie ahnungslos eine CD ins Laufwerk schieben, die Ihre Freundin Ihnen mitgegeben hat. Ein kurzer Moment der Unachtsamkeit kann Ihre gesamte Sicherheitsvorsorge gefährden. Um dies zu vermeiden, wurden wir kostenlos von unserer Beratungsfirma geschult, hellhörig zu werden und uns sicherheitsbewusst zu verhalten.

Die Etablierung einer zentralen Firewall für alle Einrichtungen war auch von den Kosten her eine vernünftige Entscheidung, denn zusätzliche Firewalls in den anderen Betriebsteilen entfielen damit. Abgerechnet wird über eine monatliche Pauschale. Hierin sind alle Leistungen enthalten, die wir

benötigen, um unsere Kommunikationswege sicher und verfügbar zu halten. Hard- und Software, Mitarbeiterschulungen, Updates und vor allem der technische Support. Wenn es irgendwo hakt, rufen wir einfach bei unserer Beraterfirma an. Unser dortiger Systemtechniker klinkt sich über einen gesicherten Internetzugang ein, um eine Ferndiagnose zu stellen und die Störung sofort zu beheben.

Wirtschaftlich und sicher

Wir wollen uns weiterhin auf unsere Arbeit am Menschen konzentrieren, statt zu IT-Experten zu werden. Aus diesem Grunde haben wir den Dienstleister auch darum gebeten, im Rahmen der Monatspauschale die Funktion des Datenschutzbeauftragten mit zu übernehmen. Für alle Beteiligten ist dies die wirtschaftlichste und sicherste Lösung.

Zusammenfassend können wir sagen, dass die Absicherung unserer neuen Kommunikationswege viel einfacher war und problemloser von statten ging als wir uns das ausgemalt hatten. Gern geben wir unsere Erkenntnisse an interessierte Schwesternschaften weiter und diskutieren Möglichkeiten einer Zusammenarbeit mit dem Ziel, unsere Infrastruktur und die Serviceleistungen auch für andere Schwesternschaften verfügbar zu machen. •

Im Haus der Hamburger Schwesternschaft haben die Computer Alarmanlagen.