HINTERGRUND

Der Newsletter der HINT AG

«Cyberrisiken muss man heute ernst nehmen und rechtzeitig für eine passende Lösung sorgen – vor allem im Interesse der Patienten und Klienten.»

**TOPTHEMA**
COMPUTERVIREN IM GESUNDHEITSWESEN

Computerviren im Gesundheitswesen

# Vorbeugen ist besser als Heilen

Unlängst haben Hackerangriffe einmal mehr für Schlagzeilen gesorgt – diesmal im Umfeld des Gesundheitswesens, insbesondere in Deutschland, in den USA und nun auch in der Schweiz. Man wähnte sich in der Schweiz bisher aus vielen Gründen besonders sicher, doch der Schein trügt: Cyberrisiken halten sich nicht an Landesgrenzen. Im Security Operation Center (SOC) der HINT AG weiss man um die Cyberrisiken und ganz besonders um die Folgen für Institutionen des Gesundheits- und Sozialwesens.

Zu Viren hatten wir schon immer ein zwiespältiges Verhältnis, so auch zu den ersten digitalen Viren, die mit dem World Wide Web aufkamen, und sowieso zu ihren neusten Varianten: den Cryptoviren. Sie sind nicht wählerisch und befallen jedes System, zu dem sie Zugang finden. Sie gefährden die Datensicherheit auf eine Weise, die nicht nur bemühend, sondern ausgesprochen schädlich ist. Doch wie es Urs Achermann, Chief Security Officer der HINT AG, trefflich ausdrückt: «Der Blitz kann überall einschlagen», weshalb die mediale Thematisierung ein nur verzerrtes Bild der tatsächlichen Bedrohungslage vermittelt.

Cyberrisiken werden für gewöhnlich als externe Bedrohungen wahrgenommen, was nur teilweise richtig ist, weil sie der unfreiwilligen Unterstützung der IT-Systeme und sogar der Anwender bedürfen. Deshalb betreffen Cyberrisiken sowohl die Sicherheit als auch den Schutz der Daten. Stichworte dazu: Gesundheitsdaten, und somit auch Patientendaten, unterstehen dem Arztgeheimnis. Als ICT-Spezialist für das Gesundheits- und Sozialwesen betreibt die HINT AG ein ständig wachsendes Security Operation Center (SOC), das laufend mit den Anforderungen und den Bedrohungen der digitalen Zeit Schritt hält. Wie hoch die Anforderungen an ein SOC inzwischen sind und wie Kunden von einer professionellen SOC-Infrastruktur profitieren können, lässt sich anhand der modernen Cyberrisiken aufzeigen.

# Prävention ist alles: Patientendaten wirksam schützen

In Deutschland wurden Kliniken von Computerviren angegriffen, in Kalifornien wurde das System eines Spitals sogar während sechs Tagen völlig blockiert und deutsche Online-Apotheken wurden erpresst. Das alles spielt sich im Ausland ab – also Entwarnung für Schweizer Institutionen des Gesundheitswesens? Nein, denn Computerviren scheuen keine Landesgrenzen, wie Medienberichte bezeugen. Deshalb ist Vorbeugen besser als Heilen – und HINT AG hat die richtigen Rezepte.

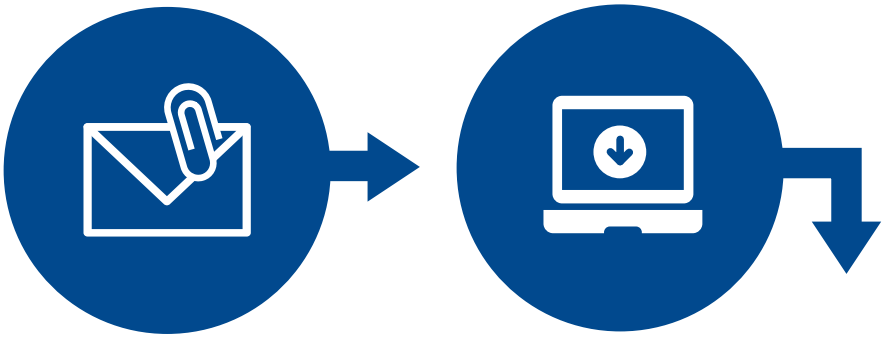
Es ist der Albtraum eines jeden IT-Verantwortlichen, wenn sein IT-System nicht mehr so funktioniert, wie es eigentlich sollte. Denn heute soll möglichst alles digital verfügbar und vernetzt sein. Die enormen Vorteile liegen klar auf der Hand, die zunehmende Abhängigkeit allerdings auch. Wie jede Technik weisen auch IT-Systeme ihre Tücken auf. Diese vorwegzunehmen heisst, sie beim Auftreten rasch zu identifizieren und zu beseitigen. Wenn aber Computerviren den Zugang zu einem IT-System finden, gilt höchste Alarmstufe. Zwar erkennen, analysieren und bekämpfen Antivirenprogramme unbefugte Eindringlinge. Bis es aber so weit ist, braucht es seine Zeit – Zeit, in der sich ein neuer Computervirus so richtig austoben kann.

### Cryptoviren – gut getarnt und besonders perfide

Cryptoviren finden verschiedene Wege, um auf den Computer eines Opfers zu gelangen. Dabei sind vor allem zwei Methoden üblich: via E-Mail mit verseuchtem Anhang (z. B. einem Word-Dokument) oder mit einem Link auf eine verseuchte Website. Die zweite Methode: Der Virus


**Die Presse kann auf Risiken hinweisen, die sich bereits verwirklicht haben – die Prävention von Cyberrisiken setzt jedoch viel früher an.**

**Den Artikel aus dem Tages-Anzeiger können Sie unter folgendem Link nachlesen:**
http://www.tagesanzeiger.ch/schweiz/standard/patientendaten-sind-oft-leichte-beute/story/30366313



SPAM-Mail mit Malware oder
Webseite mit Malware

Malware ist auf dem Zielcomputer,
lädt neue Module und den
starken Schlüssel vom C2C Server herunter

Benutzer muss Lösegeld bezahlen
(Bitcoins, via TOR Netzwerk verschleiert)

Malware hinterlässt eine Erpresser-
Botschaft mit Ablaufdatum

Malware verschlüsselt alle
Daten des Benutzers

verteilt sich selber auf einer gehackten Website via sogenannte «Drive-by-downloads», die über eine Sicherheitslücke auf dem Computer des Anwenders ins eigene IT-System eindringen.

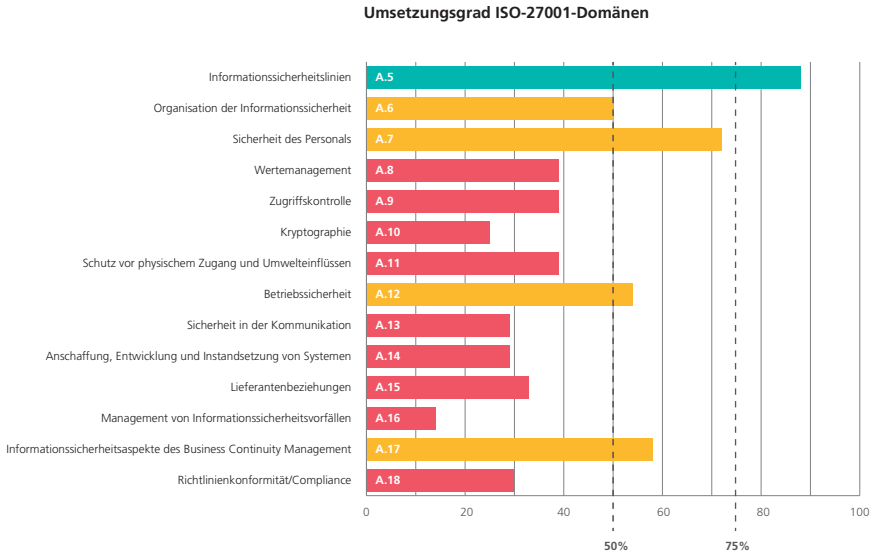
Cryptoviren gelangen also wie die meisten Computerviren auf bekannten Wegen in ein IT-System. Sind sie einmal drin, gehen sie systematisch zu Werke: Zuerst verbindet sich ein Cryptovirus mit einem C2C-Server (Command and Control Server) und meldet seine Bereitschaft, auf dem Zielrechner Dateien zu verschlüsseln. Der C2C-Server erstellt und übermittelt daraufhin einen starken Schlüssel. Was nun folgt, ist offensichtlich: Mit dem starken Schlüssel beginnen Cryptoviren alle Dateien zu verschlüsseln und sie damit dem Zugriff des Anwenders zu entziehen. Je umfassender die Befugnisse auf dem befallenen Anwendersystem sind, desto weitreichender ist auch der Zugriff der Cryptoviren.

### Was das für das Gesundheitswesen bedeutet

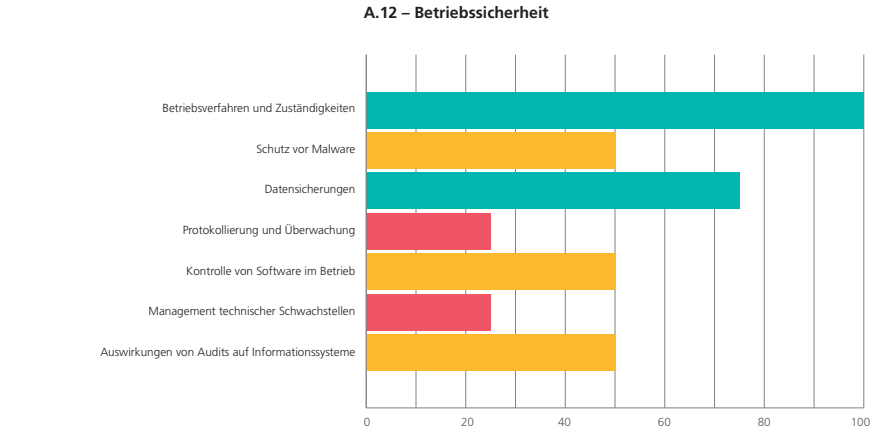
Wie die Zugangswege bereits verraten, sind Cryptoviren nicht auf ein bestimmtes Land oder eine Landessprache beschränkt und was sie tun, tun sie branchenunabhängig – sie verschlüsseln jeden beliebigen Informationsgehalt von Files einfach nur anhand des Dateienformats. Und weil weder der betroffene Anwender noch der IT-Verantwortliche den verwendeten Schlüssel kennt, entziehen sich die verschlüsselten Dateien ihrem Zugriff. Für ein Unternehmen, das nicht mehr auf Kunden-, Personal-, Bestell-, Inventar- oder Buchhaltungsdaten zugreifen kann, ist das schlicht eine Katastrophe. Für Spitäler und Kliniken bedeutet das darüber hinaus, dass sie nicht mehr auf KIS und PACS zugreifen können, auf MRI-Aufnahmen oder Vitaldatenverläufe – die Gesundheit oder gar das Leben von Patienten ist in Gefahr. Von daher erstaunt es nicht, dass Institutionen des Gesundheitswesens auf den Erpresserzweck solcher Cryptoviren eingehen und dafür bezahlen, den Schlüssel für die verschlüsselten Dateien zu erhalten.

### Der Schutz vor Cryptoviren folgt dem Schutz vor Cyberrisiken

Sieht man von den besonderen Auswirkungen von Cryptoviren ab, sind auch sie letztlich «nur» Computerviren und somit Teil der Cyberrisiken, die mit der wachsenden Digitalisierung und Vernetzung einhergehen. Bereits mit den bestens bekannten, bewährten, aber noch nicht überall beherzigten organisatorischen und




**Security Quick Assessment: Mögliche Übersicht über den Umsetzungsgrad in allen ISO-Domänen.**




**Security Quick Assessment: Mögliche Übersicht über den Umsetzungsgrad im Bereich «Betriebssicherheit»**

technischen Schutzmechanismen kann vielen Cyberrisiken vorgebeugt werden: Dazu zählt die Schulung und laufende Sensibilisierung der Mitarbeitenden im Umgang mit E-Mails und im WWW – das Wissen darum, was eine verdächtige Mailbeilage sein könnte, und eine gebotene Zurückhaltung beim Surfen auf externen Websites. Auch ein durchdachtes «Rollen- und Berechtigungskonzept» trägt dazu bei, dass Mitarbeitende über alle für ihre Tätigkeit benötigten Zugriffsberechtigungen verfügen, aber nicht mehr. Und last but not least: Wichtig sind bedarfsgerechte und gut geschützte Backups für jede denkbare und undenkbare Eventualität – zum Beispiel, um von Cryptoviren verschlüsselte Dateien zu ersetzen.

## Maximaler Schutz dank Outsourcing an HINT AG

Ein wirksames Sicherheitskonzept basiert auf Professionalität. Die HINT AG betreibt ein nach ISO 27001 zertifiziertes Security Operation Center (SOC), das ständig den aktuellsten Anforderungen angepasst und ausgebaut wird. Ein solches SOC sprengt jedoch die Möglichkeiten von kleinen und mittleren Institutionen des Gesundheits- und Sozialwesens in mehrfacher Hinsicht. Aber auch grössere Institutionen stehen vermehrt vor dem Dilemma, sich für wachsende Investitionen in das eigene SOC oder die eigenen Kerntätigkeiten zu entscheiden. Für die HINT AG zählt das SOC zu einer ihrer Kernkompetenzen. Kunden der HINT AG, die sich für ein Outsourcing entschieden haben, können alle damit zusammenhängenden Dienstleistungen beanspruchen. Mit einem Security Quick Assessment zeigt die HINT AG dem interessierten Management auf, wie die eigene Institution aktuell bezüglich IT-Sicherheit nach ISO 27001 unterwegs ist. Das Assessment wird auf Interview-Basis durch erfahrene Sicherheitsexperten vor Ort durchgeführt.

Das HINT-Team arbeitet mit Überwachungstools, welche die Log- und System-Informationen vieler IT-Systeme in Echtzeit zentral sammeln und auswerten. So werden alle verdächtigen Internetzugriffe und ungewöhnliche Aktivitäten auf den Dateiservern analysiert. Mit dem SOC-Team haben die Spezialisten von der HINT AG im August 2015 den ersten Cryptovirus-Befall bei einem Kunden entdeckt und die Gefahr frühzeitig gebannt. Wie zeitkritisch Sofortmassnahmen sind, verdeutlichen zwei Praxisbeispiele: Bei einem Vorfall mit einem Cryptovirus wurden innerhalb von 20 Minuten rund 20 000 Dateien verschlüsselt, bei einem anderen Fall waren es über 140 000 Dateien innerhalb von weniger als einer Stunde. Cyberrisiken sind auch für die Schweiz durchaus real und Cryptoviren sowieso – mit einem professionellen Partner an Ihrer Seite sind beide beherrschbar.

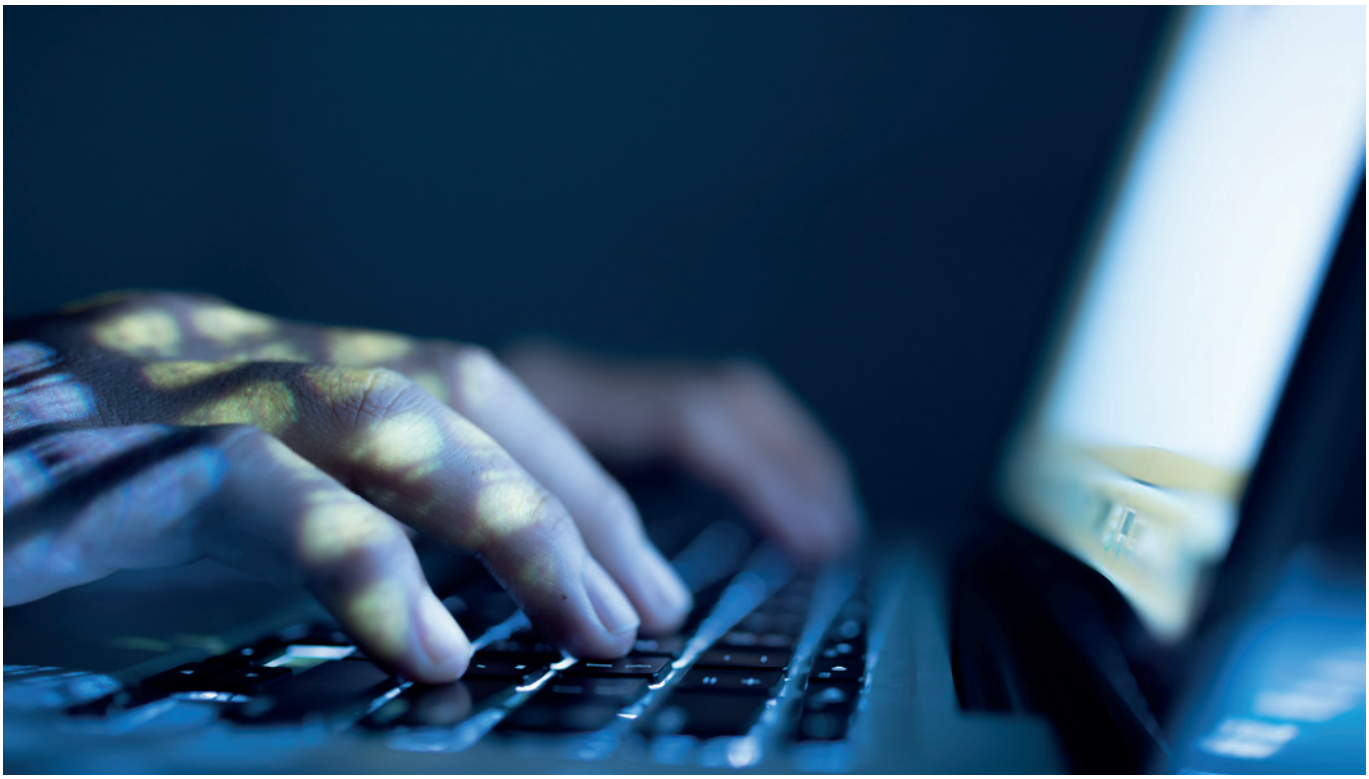
# Cyberrisiken und Datenschutz

In Bezug auf die digitalen Gefahren von aussen, aber auch von den Anwendern selbst gilt es im Gesundheits- und Sozialwesen Aspekte zu beachten, die in anderen Branchen weniger im Fokus stehen: Es geht praktisch immer um Patienten- und Klientendaten, die der Gesetzgeber bewusst zu «besonders schützenswerten Personendaten» erklärt hat.

Neben allen technischen und organisatorischen Aspekten gilt es im Gesundheitswesen ein besonders wichtiges Element zu beachten: das Arztgeheimnis, das immer dann in Gefahr ist, wenn sich Cyberrisiken verwirklichen. Bei den beschriebenen Cryptoviren droht diese Gefahr nicht – noch nicht, denn statt die Daten nur zu verschlüsseln und gegen ein Lösegeld wieder freizugeben, könnten sich die Cyberkriminellen die verschlüsselten Daten auch zusenden. Welchen Einfluss das auf die Höhe des Lösegeldes hätte, ist unbekannt, der dadurch angerichtete Schaden wäre auf jeden Fall erheblich.

Seitens der Anwender ist klar, dass die elektronischen Medien den Austausch von Patienten- und Gesundheitsdaten sowie von Bilddateien wesentlich vereinfachen und beschleunigen. Diesen Vorzügen stehen aber die gesetzlichen Vorgaben sowie die berechtigten Patienten- und Klienteninteressen gegenüber, denn Daten über die Gesundheit oder über Massnahmen in der sozialen Hilfe gelten als besonders schützenswerte Personendaten. Zudem unterstehen unter anderem Ärzte, Zahnärzte, Chiropraktiker, Apotheker, Hebammen und Psychologen dem Berufsgeheimnis.

**Was bedroht das Berufsgeheimnis?**
Die digitale Technik kennt kein Berufsgeheimnis und unterscheidet auch nicht, welches Bit oder Byte nicht schützenswert, gewöhnlich oder besonders schützenswert ist – diese Aufgabe fällt den Anwendern zu und beginnt beim Praxiscomputer: Wer kann auf die darauf gespeicherten Patientendaten mit oder ohne Berechtigung zugreifen, wer das Backup in der Cloud oder beim Provider abrufen? Hier unterscheiden sich die Themen Datensicherheit und Datenschutz. Soweit es das praxiseigene IT-System angeht, ist es im Ergebnis einerlei, ob ein ausgeklügelter



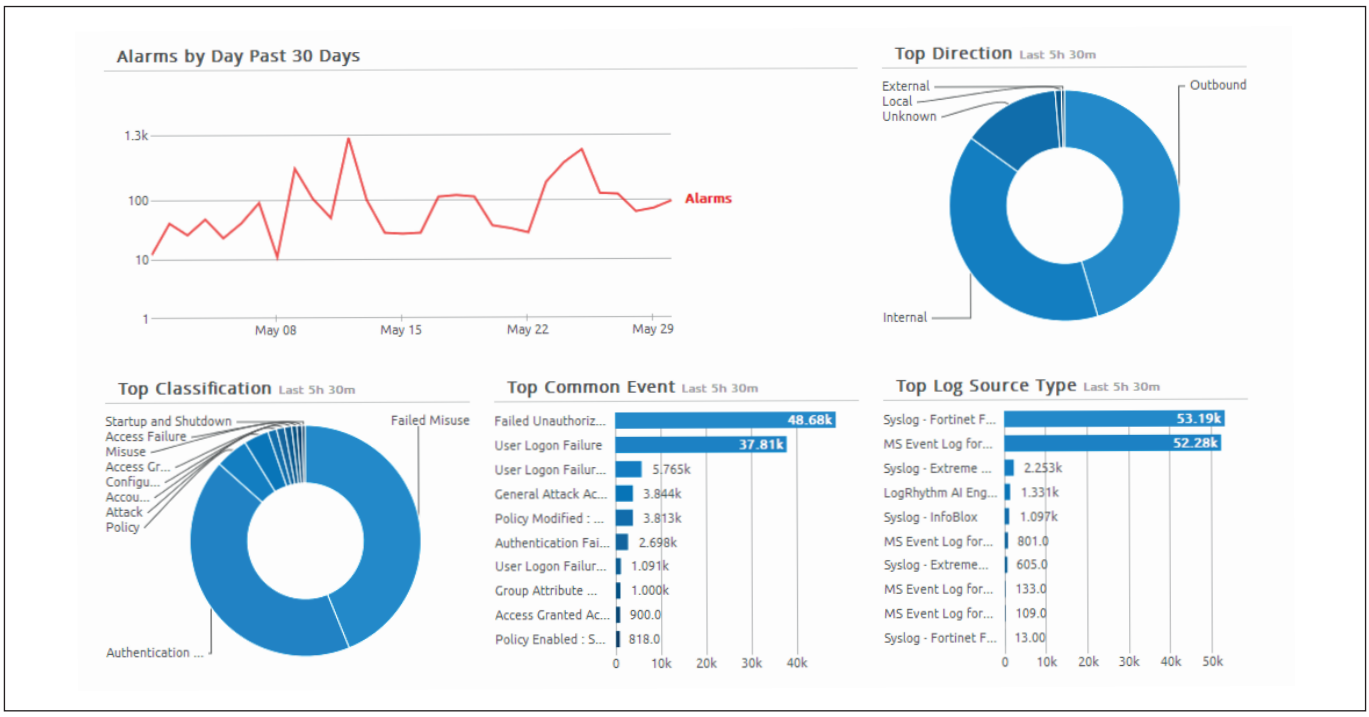
**Das Gesundheits- und Sozialwesen ist bei der Datensicherheit und ganz besonders beim Datenschutz gefordert – im Interesse der Patienten und Klienten.**

Hackerangriff, ein Einbrecher oder ein Unbefugter sich der Daten auf dem Praxisrechner bemächtigt – das Berufsgeheimnis ist auf jeden Fall bedroht.

Die andere Bedrohung für das Berufsgeheimnis geht vom berechtigten Anwender aus: Eine kurze E-Mail-Anfrage mit Daten, die via Copy/Paste samt Patientennamen eingefügt werden, eine zu ausführliche Datei als Beilage, eine Röntgenaufnahme sie den Empfänger erreicht. Die Frage, ob das Berufsgeheimnis dadurch nur bedroht oder verletzt wurde, erübrigt sich.

## HINT AG unterstützt mit Einzel- und Gesamtlösungen

Will man den statistischen Erhebungen glauben, ist es mit dem Datenschutz im Schweizer Gesundheits- und Sozialwesen eher schlecht bestellt. Viele wissen oder ahnen, dass nicht jede Praktik dazu taugt,




**Dashboard eines Security Analysten des Security Operation Center (SOC): Alles auf einen Blick**

via WhatsApp, eine grössere Datei über Dropbox usw. Was auch immer ungeschützt bzw. unverschlüsselt elektronisch übermittelt wird, muss den Vergleich mit der Postkarte aus den Ferien nicht scheuen: Solange die Postkarte unterwegs ist, kann sie von jedermann gelesen werden. Immerhin folgt die Postkarte einem einigermassen direkten resp. vorgegebenen Weg zwischen Absender und Empfänger. Die elektronische Mitteilung hingegen wird von einem unbekannten Server zum nächsten weitergereicht und kann durchaus alle fünf Kontinente besucht haben, bevor den besonders schützenswerten Patienten- und Klientendaten zu genügen. Sie laufen damit Gefahr, ihr Berufsgeheimnis zu verletzen. Als ICT-Spezialistin im Gesundheits- und Sozialwesen wissen die Spezialisten der HINT AG, dass gute Lösungen vorhanden sind – sie bieten für jeden Bedarf geeignete Einzel- und Gesamtlösungen aus einer Hand. Somit bleibt nur die Empfehlung, die Cyberrisiken ernst zu nehmen und rechtzeitig für eine passende Lösung zu sorgen – im eigenen wie auch im Interesse der Patienten und Klienten.

**Die digitale Welt beschreitet den Weg der Vernetzung – die Richtung geben aber die Chancen und Risiken vor.**

# Vernetzung? Ja, aber sicher!

Die Vernetzung der digitalen Welt ist ein folgerichtiger und auch wegweisender Schritt. Welche heute angestrebten Ziele tatsächlich auch erreicht werden, steht allerdings auf einem anderen Blatt. Denn für alles Neuartige gilt, dass auch der Weg Teil des Zieles ist.

Nimmt man die autonome Automobiltechnik oder die Gebäudeautomation als Vorboten, dann zeichnet sich ab, dass wir noch ganz am Anfang der Vernetzungsmöglichkeiten stehen. Wenn ein Herzschrittmacher automatisch meldet, dass etwas nicht mehr stimmt, kann das lebensrettend sein. Dieselbe Vernetzung macht das Gerät aber auch angreifbar. Die Vorzüge einer weiteren Vernetzung sind offensichtlich, die Risiken allerdings auch.

Gleichzeitig wird sich der Datenaustausch deutlich intensivieren. Treiber dafür sind die stark wachsende Datenmenge, immer raffiniertere bildgebende Verfahren und die verstärkte interdisziplinäre Zusammenarbeit der Leistungserbringer. Weiter ist auch das elektronische Patientendossier zu nennen, für dessen Einführung verschiedene Kantone mit ihren Communities schon wertvolle Vorarbeit geleistet haben.

Mehr Vernetzung und Datenaustausch zeigen, wie entscheidend wirksame Massnahmen zur Datensicherheit und damit auch zur Bewahrung der Integrität von Patienten und Versicherten sind. Die Spezialisten der HINT AG beraten Institutionen des Gesundheitswesens individuell und praxisnah.


## HINT AG PROVIDER, CONSULTANTS UND INTEGRATOREN – DIE BEHANDLUNG BEGINNT BEIM PATIENTEN

Die 110 Fachleute der HINT AG vernetzen Akteure, Infrastruktur, Portale und Service-Desk-Lösungen für Prozesse und persönliche Gesundheits- und Patientendaten in der Schweiz. Die Spezialisten sind zur Stelle: von der Konzeption bis zur Implementierung sorgfältig evaluierter Lösungen. Dank des breiten sowie tiefen Know-hows kommen Kunden schneller ans Ziel. Dafür sorgen auch Partnerschaften mit führenden Unternehmen.
Das solide Fundament der HINT AG Services bilden drei starke Säulen:

### › IT Service Provider – kalkulierbar, skalierbar und flexibel

IT-Lösungen werden kalkulierbar, skalierbar und flexibel dank garantierter Technologie-Transformation. Die hochsichere HINT AG Cloud ermöglicht jegliche Applikation als Service zu beziehen.

### › IT Consulting Partner – sicher, stabil und geschützt

Die HINT AG bietet patientenzentrierte Informationen für patientenzentrierte Entscheidungen auf Basis eines ISO-27001-geprüften Informationssicherheitsmanagements sowie von hochsicheren und hochverfügbaren Rechenzentren. Mit der hohen Kompetenz im Bereich IHE und EPDG führt HINT AG ihre Kunden auf sicherem Weg zum ePatientendossier. Umfassende Visual Analytics sorgen für den nächsten Level, ein umfassendes Analyse Cockpit für zentrale unternehmensstrategische Entscheidungen.

### › IT Solution Integratoren – innovativ und qualitätsorientiert

Fortschrittliche und nachhaltige Lösungen führen zur Verbesserung der medizinischen Behandlungskette.
Die nutzerorientierte Gestaltung und Einbindung von Informationsquellen, die Einbindung von Portalen und Apps für bürgerzentrierte Applikationen sind zukunftsweisende Dienstleistungen der HINT AG. Sie sorgen für eine moderne integrierte Versorgung unter dem steten Fokus: Die Behandlung beginnt beim Patienten.

**Herausgeber**

HINT AG
Niederlenzer Kirchweg 4
5600 Lenzburg
Telefon +41 58 404 57 00
Fax +41 58 404 57 01

info@hintag.ch
www.hintag.ch

**Ausgabe**
**Nr. 1/2016**

HINTAG
Health Information Technologies AG