

RISIKOANALYSE

Weshalb Kriminelle Krankenhäuser lieben



Beim folgenden Gastbeitrag handelt es sich um die Transkription eines Videobeitrags, den der Sicherheitsberater Gerhard Link auf Youtube ins Netz gestellt hat (<https://youtu.be/UrDuzjLiz7k>). Der Sicherheits-Berater kann die Erfahrungen dieses Autors durchaus bestätigen:

Gastbeitrag



Es vergeht kein Tag, an dem nichts in der Presse über das Thema Sicherheit in Krankenhäusern geschrieben steht. Angefangen vom aktuellen Topthema Cyberangriffe auf IT-Infrastrukturen bis hin zur einfachen Kriminalität, wie Einbruch, Diebstahl und Vandalismus - man findet eine ganze Palette von Angriffsmöglichkeiten. Aber was macht es für einen Kriminellen so interessant, sich ein Krankenhaus als Tatobjekt auszusuchen?

Pressethema

Ein Krankenhaus ist ein Ort, in dem Gutes getan wird und man als Mensch Hilfe erfährt. Man denkt nicht daran, dass solche Orte auch von Kriminellen aufgesucht werden. Denn wer möchte schon, dass durch kriminelle Handlungen andere Leben in Gefahr geraten können? Aber in unserer heutigen Zeit scheint es, dass Ethik, Moral und Nächstenliebe keine so große Rolle mehr spielen. Um sich persönlich zu bereichern, suchen Kriminelle heutzutage leicht angreifbare und lukrative Ziele aus, deren Verantwortliche sich bislang mit Sicherheitsthemen nicht beschäftigen mussten. Dazu zählen nun auch Krankenhäuser und Kliniken.

Psychosoziales Umfeld

Daten und Fakten:

Ob Geldbörsen, Handys, Endoskopiegeräte oder andere medizinische Geräte - in deutschen Krankenhäusern wird gestohlen, was das Zeug hält. Es gibt zwar keine bundesweite Statistik, doch welches Ausmaß die Straftaten erreichen, zeigen die polizeilichen Kriminalstatistiken der einzelnen Bundesländer.

Die neuesten Zahlen hierzu stammen aus dem Jahr 2017:

- In diesem Jahr wurden beispielweise in Nordrhein-Westfalen laut Landeskriminalamt fast 6.500 Diebstahlsfälle mit einem Schaden von 3,5 Millionen Euro in Krankenhäusern registriert. Das Jahr zuvor erreichte einen Schadensrekord von ca. acht Millionen Euro - und das bei einer nur leicht erhöhten Anzahl von Diebstählen.

3,5 Mio Euro Schaden

Tageweise Betriebsausfälle

- Hinzu kommen Sicherheitsvorkommnisse, welche teilweise Betriebsausfälle eines kompletten Klinikums über mehrere Tage verursachen, finanziell von den Krankenhäusern nicht aufgefangen werden können und nicht unbedingt durch eine Versicherung abgesichert sind.

Zusatzkosten

- Das heißt, bei einem Jahresumsatz von ca. 300 Mio. Euro entsteht bei einem Ausfall von sieben Tagen ein finanzieller Umsatzverlust von ca. sechs Millionen Euro plus zusätzliche Kosten für beispielsweise die Verlegung von Patienten in andere Krankenhäuser und Arbeitsaufwand für das Herstellen des Normalzustandes des Krankenhauses.

Öffentliche und spezielle Bereiche**Wieso geraten Krankenhäuser ins Visier von Kriminellen?**

Krankenhäuser und Kliniken sind grundsätzlich öffentliche Bereiche, in denen sich Menschen frei bewegen können. Es gibt aber auch Bereiche, in denen sich nur bestimmte Personengruppen aufhalten dürfen. Dazu zählen spezielle Klinikbereiche wie beispielsweise Operationsbereiche, Forschungsabteilungen, Behandlungsräumlichkeiten und auch Infektionsbereiche. Aber auch Bereiche, welche die technische Versorgung des Klinikums mit Strom, Klima und einiges mehr garantieren sollen.

Veraltete Bestandsgebäude

Fakt ist aber, dass große Kliniken über Jahre gewachsen sind und mittlerweile einen sehr großen Bestand an alten Gebäuden vorweisen, welche gebäudetechnisch gesehen nicht in letzter Konsequenz an die heutigen Bedürfnisse angepasst worden sind. Dies betrifft auch das Thema technische Sicherheit.

Leichter Zutritt selbst in Sicherheitsbereiche

Werden beispielsweise in Wirtschaftsunternehmen Räumlichkeiten wie Entwicklungsabteilungen als Sicherheitsbereiche angesehen und auch technisch entsprechend ausgestattet, so können dagegen Kliniken in bestimmten Sicherheitsbereichen relativ einfach von nicht autorisierten Personen begangen werden. Diese Personen werden oftmals auch nicht vom dort arbeitenden Klinikpersonal als unberechtigte Person wahrgenommen.

» Mit gestohlenen medizinischen Geräten lässt sich ein gutes

Geschäft machen. «

Dies zeigt somit, dass sich Krankenhäuser für Diebe oder andere Täter als ideales Betätigungsfeld mit einem relativ niedrigen Entdeckungsrisiko darstellen. Mit gestohlenen medizinischen Geräten lässt sich ein gutes Geschäft machen und ein Krankenhaus lässt sich auch gut erpressen.

Welche Arten von Angriffsmöglichkeiten gibt es in Krankenhäusern?

Die Angriffsmöglichkeiten in Krankenhäusern sind durchaus vielseitig. Es gibt nicht nur die eine bestimmte Bedrohung, welche grundsätzlich in Klinikbereichen zu finden ist, sondern eine ganze Palette unterschiedlicher krimineller Angriffsmöglichkeiten, z. B.:

Von Cyber- bis Aktivistenangriff

- Cyberangriffe, welche erpresserische Hintergründe oder auch Sabotagegründe haben
- Diebstähle medizinischer Geräte, wie beispielsweise Endoskope
- allgemeine Diebstähle wie Handys, Geldbörsen und vieles mehr
- Sabotage von technischen Anlagen, um den Krankenhausbetrieb lahmzulegen
- Vandalismus, wie beispielsweise eine eingetretene Tür oder eingeschlagenes Fenster
- Gewaltbereitschaft von Patienten und Familienangehörigen in Ambulanzen
- Wirtschaftsspionage in Forschungsabteilungen
- Aktivistentätigkeiten, z. B. in Tierforschungsbereichen

Es ist schon erschreckend, welche Möglichkeiten ein Krankenhaus für einen Kriminellen bieten kann, um sich zu bereichern, und wie schutzlos manche Kliniken dem gegenüberstehen.

Wie einfach ist es denn, in bestimmte Krankenhausbereiche einzudringen?

Durch den öffentlichen Charakter kann man sich in Krankenhäusern überall bewegen und aufhalten. Normalerweise gibt es in Krankenhäusern und Kliniken Besuchszeiten, welche auch eingehalten werden sollten. Außerhalb dieser Besuchszeiten sind Besuche nur bei Schwerkranken und in besonderen Fällen möglich.

Allerdings werden Besucher, welche sich auch außerhalb der Besuchszeiten noch in Krankenhausbereichen aufhalten, oftmals nicht kontrolliert. Das Pflegepersonal ist neben seiner eigentlichen Aufgabe, sich um die Patienten zu kümmern, nicht in der Lage, Kontrollaufgaben zu übernehmen.

Besucher, welche sich in den Abendstunden über eine Sprechanlage am Nachteingang eines Krankenhauses beim Pflegepersonal melden, werden in der Regel mittels Türöffner hereingelassen, aber nicht am Nachteingang in Empfang genommen und eskortiert.

So entstehen Sicherheitslücken, welche von Kriminellen sehr gerne genutzt werden. Auch sind ältere Klinikgebäude, aber auch neue Klinikkomplexe, gar nicht oder nur wenig mit Sicherheitstechnik ausgestattet. Somit ist es für Einbrecher besonders leicht, in Gebäude einzudringen. Der eingesetzte Sicherheitsdienst, welcher einen Klinik-campus mit über 30 Gebäuden überwachen soll, ist bei solchen minimalst ausgestatteten Gebäuden nicht in der Lage, für einen entsprechenden Schutz zu sorgen. Manchmal läuft die Entdeckung einer Straftat auf einen Zufall hinaus - der Sicherheitsdienst ist gerade da vor Ort, wo etwas passiert. Die Aufdeckung ist also reine Glückssache.

Das Gleiche gilt auch im Bereich der IT-Sicherheit. Neben neuen Softwaresystemen werden beispielsweise auch noch alte Systeme im gleichen Netzwerk betrieben. Da es für die älteren Systeme keine Sicherheitsupdates mehr gibt bzw. vergessen wird, neue aufzuspielen, entstehen Sicherheitslücken, welche von einem Hacker gerne genutzt werden, um das System mit Schadsoftware zu infiltrieren.

Was können Krankenhäuser für die Sicherheit tun?

Entdeckte Sicherheitslücken einfach zu stopfen reicht nicht aus, denn da, wo die Lücke ist, liegt in der Regel nicht die Ursache. Man hinkt immer den Sicherheitsvorkommnissen hinterher und vergeudet dabei viel zu viel Zeit und Geld. Viel wichtiger ist es, nach der Ursache zu suchen und systematisch die daraus möglichen Sicherheitslücken, bevor sie eintreten, zu eliminieren. So etwas nennt man Prävention!

Im Medizinischen beispielsweise findet die Prävention eine besondere Beachtung. Durch vorbeugende Maßnahmen möchte man den Eintritt einer Krankheit verhindern, verzögern oder auch mögliche Krankheitsfolgen abschwächen. Vor diesem Hintergrund mutet es schon komisch an, dass Krankenhäuser, welche die medizinische Prävention kennen und ausüben, der Vorsorge für das wirtschaftliche Überleben des Krankenhauses wenig Aufmerksamkeit schenken.

Sicherheitskonzepte für Kliniken oder Krankenhäuser wären in erster Linie das Richtige. Diese beschreiben Sicherheitsstandards, die notwendig sind, um ein entsprechendes Maß an Sicherheit zu gewährleisten - ob sie sich nun technisch, organisatorisch oder personell darstellen.

» Der Sicherheitsdienst kann nicht für entsprechenden Schutz sorgen.«

Während der Besuchszeiten**Kaum Zeit für Kontrollen****Türöffner ohne Eskorte****Aufdeckung Glückssache****Sicherheitslücken in der IT****Ursachenforschung bei Sicherheitslücken****Missachtung der Präventionsphilosophie****Sicherheitskonzepte für Sicherheitsstandards**

Planung der Sicherheitstechnik

Diese Konzepte verhindern beispielsweise den Sicherheitswildwuchs beim Bau von Klinikgebäuden. D. h., durch gut geplante und eingesetzte Sicherheitstechnik in Kombination mit der entsprechenden Nutzung eines Gebäudes entsteht ein einheitliches Sicherheitsniveau, das von allen Beteiligten, wie zum Beispiel dem Sicherheitsdienst, gut, einfach und strukturiert gehandelt werden kann. Es gibt somit nicht mehr so viele Insellösungen und verschiedene Vorgehensweisen in Punkto Sicherheit.

Fazit:

So, wie es für einen Menschen wichtig ist, zu Vorsorgeuntersuchungen zu gehen, um frühzeitig gegen mögliche Erkrankungen einwirken zu können, ist es auch in wirtschaftlichen Bereichen wichtig, für das Überleben eines Unternehmens wichtige vorsorgliche Maßnahmen zu treffen.



Der Gastautor Gerhard Link

Strategische Sicherheitsberatung in der Unternehmenssicherheit, in Tourismus- und Privatbereichen, technische und organisatorische Sicherheit, Sicherheitsanalysen, Sicherheitskonzepte, Projektmanagement bei Sicherheitsprojekten

Fragen an unseren Gastautor? g.link@gerhardlink.com

IT-WIRTSCHAFTLICHKEIT

Abwärmennutzung im Rechenzentrum

Wunschvorstellung

Im Idealfall sollte man bei jedem RZ-Neubau zusätzlich ein Schwimmbad errichten. Warum? Um direkt und effektiv die IT-Abwärme nutzen zu können. Leider ist der Bedarf an Schwimmbädern bei Unternehmen, die eigentlich ihre IT auf ein starkes Fundament stellen wollen, selten gegeben. Aber Spaß beiseite, was soll diese Wunschvorstellung verdeutlichen?

Nutzungs- voraussetzungen?

Für eine wirtschaftliche Nutzung der IT-Abwärme, die über das Jahr gesehen konstant Abwärme produziert, müsste auf der anderen Seite der ganzjährige Bedarf an entsprechender Heizenergie bestehen. Das würde z. B. bei Nah- und Fernwärmenetzen, aber auch für die oben genannten Schwimmbäder, zutreffen. Meist sind diese jedoch nicht vorhanden oder befinden sich zu weit weg. Aber auch das überwiegend zu geringe Temperaturniveau der Abwärme stimmt nicht mit der Nutzerquelle überein. Nimmt man

beispielsweise ein luftgekühltes Rechenzentrum mit heute gängigen Zulufttemperaturen um ca. 24 Grad Celsius und den entsprechenden Rücklufttemperaturen von ca. 30 Grad, dann ergeben sich potenziell nutzbare Wassertemperaturen im selben Bereich. Die Nutzung für direkte Heizzwecke ist somit fast ausgeschlossen.

Im High Performance Computing, kurz HPC, sind bei direkter Abwärmennutzung durch Flüssigkeitskühlung weit höhere Temperaturen von ca. 40 bis 60 Grad Celsius möglich. Hier wird eine direkte Heizungsunterstützung eher in Frage kommen - vorausgesetzt sie ist vorhanden und auch ganzjährig nutzbar.

