Der falsche Techniker â?? Wenn der Zugang zum Herzen der Klinik fÃ¼hrt

Wenn Sicherheit kein Thema ist â?? wird sie zum Risiko

In Kliniken ist das Thema â??Sicherheitâ?? fÃ¼r die meisten Mitarbeitenden â?? ob im Pflegedienst, in der Technik oder Verwaltung â?? **kein Teil des beruflichen Alltags.** Die Aufmerksamkeit liegt verstÃ¤ndlicherweise auf Patientenversorgung, Funktionserhalt und operativer Organisation. Sicherheitsdenken, wie es in Industrieanlagen oder BehÃ¶rden lÃ¤ngst zum Standard gehÃ¶rt, ist in vielen KrankenhÃ¤usern **nicht verankert â?? weder im Bewusstsein noch in den AblÃ¤ufen.**

Â© Security Explorer

Die meisten BeschÃ¤ftigten in einem Klinikum haben nie eine systematische Sicherheitsunterweisung erhalten. Begriffe wie Zutrittsberechtigung, TÃ¤terprofile, RollentÃ¤uschung oder manipulative Handlungen sind ihnen weitgehend fremd.

Das ist kein persÃ¶nliches VersÃ¤umnis â?? sondern ein strukturelles.
Denn Ã¼ber Jahrzehnte galt das Krankenhaus als â??offenes Systemâ?? â?? ein Ort des Vertrauens, nicht des Verdachts.

Doch genau das macht es heute besonders anfÃ¤llig. Mit dem **KRITIS-Dachgesetz**, das fÃ¼r Kliniken als kritische Infrastrukturen verbindliche Anforderungen an Sicherheit und Resilienz festlegt, **Ã¤ndert sich diese Ausgangslage grundlegend.**

Wo frÃ¼her Routine war, muss kÃ¼nftig Sicherheitsbewusstsein herrschen.
Und wo bisher auf Vertrauen gebaut wurde, braucht es **klare Prozesse, Nachweise und Kontrolle.**

Ein realer Vorfall zeigt exemplarisch, wie gravierend die Folgen ausbleibender Sicherheitskultur sein kÃ¶nnen â?? **ganz ohne Gewalt, einfach durch TÃ¤uschung und SystemlÃ¼cken.**

Das Szenario: Der vermeintliche Servicetechniker

Ein Mann meldet sich am spÃ¤ten Vormittag an der Klinikpforte. Er trÃ¤gt eine Jacke mit dem Logo der Stadtwerke, nennt einen Ansprechpartner und gibt an, eine planmÃ¤Ã?ige Wartung in der Wasserversorgungszentrale durchfÃ¼hren zu mÃ¼ssen. Die Anmeldung informiert den technischen Dienst, der aufgrund der Routine nicht weiter prÃ¼ft. Der Mann erhÃ¤lt eine **elektronische Zutrittskarte** â?? mit Zugriff auf **alle technischen Infrastruktur-RÃ¤ume im Haus.**

Ein Mitarbeiter begleitet ihn zur Wasserversorgung â?? der zugewiesene Einsatzort. Nach einem kurzen GesprÃ¤ch und dem Start seiner â??Arbeitenâ?? **lÃ¤sst man ihn allein zurÃ¼ck.**

TatsÃ¤chlich ist der Mann **kein echter Techniker**, sondern ein TÃ¤ter, der gezielt Zugang zu den Versorgungssystemen erschleichen wollte. WÃ¤hrend er unbeobachtet arbeitet, **Ã¶ffnet er mit seiner Karte auch die benachbarte Klima- und LÃ¼ftungszentrale** und manipuliert dort eine Steuerungseinheit. Der Sabotageeffekt ist zeitverzÃ¶gert: Erst nach etwa **90 Minuten** fÃ¤llt die komplette LÃ¼ftungsversorgung aus.

Erst als mehrere OP-SÃ¤le nicht mehr belÃ¼ftet werden kÃ¶nnen und die Klimatisierung auf Isolierstationen versagt, schlÃ¤gt das System Alarm. Der TÃ¤ter ist da lÃ¤ngst verschwunden.

Analyse: Wo das System versagt hat

Schwachstelle	Beschreibung
Keine PrÃ¼fung der IdentitÃ¤t	Der TÃ¤ter wurde auf Basis von Auftreten und Kleidung akzeptiert â?? ohne Dokumentations- oder Ausweiskontrolle.
Unkritische Zutrittsvergabe	Die ausgestellte Zutrittskarte ermÃ¶glichte Vollzugriff â?? anstatt auf den konkreten Einsatzort beschrÃ¤nkt zu sein.
Keine Begleitung im sensiblen Bereich	Nach kurzer Einweisung wurde der externe â??Technikerâ?? alleine gelassen â?? ohne Aufsicht.
Keine InnenÃ¼berwachung	Weder Kameras noch Bewegungsmelder erfassten die Manipulation.
VerzÃ¶gerte Auswirkung â?? verzÃ¶gerte Reaktion	Die Sabotage war bewusst so angelegt, dass sie erst nach Stunden sichtbar wurde â?? die TÃ¤teridentifikation war zu spÃ¤t.

Das strukturelle Problem: Vertrauen ersetzt keine Sicherheitsstrategie

Â© Security Explorer

Dieser Vorfall verdeutlicht ein Muster, das in vielen Kliniken anzutreffen ist:

- Zutritt wird nach Bedarf vergeben â?? nicht nach Rollenprofil.
- Technische Infrastrukturbereiche gelten als â??sicherâ??, da sie selten betreten werden.
- Externe mit technischem Auftreten werden **nicht kritisch hinterfragt.**
- Es fehlt ein Bewusstsein fÃ¼r das **Manipulationspotenzial im Inneren.**

Mit dem **KRITIS-Dachgesetz** ist dieses Verhalten nicht nur risikobehaftet â?? **sondern rechtswidrig.** Denn Kliniken mÃ¼ssen nachweislich in der Lage sein, physische wie digitale Angriffe zu verhindern, frÃ¼hzeitig zu erkennen und deren Auswirkungen zu minimieren.

Empfehlungen zur StÃ¤rkung der Sicherheit in Technikbereichen

1. Zutritt nur mit Legitimation und Rollenprofil

- Keine Karten mit Vollzugang
- Zutritt auf Raum und Zeit beschrÃ¤nken (â??Need-to-accessâ??)
- Bewegungsprotokolle bei Fremdfirmen verpflichtend

2. Begleitpflicht fÃ¼r externe Dienstleister

- Kein unbeaufsichtigter Aufenthalt in Versorgungszentralen
- Kontrollprotokolle: Wer hat was gemacht â?? wann â?? mit wem?

3. RaumÃ¼berwachung und Manipulationserkennung

- PrÃ¤senzsensorik in technischen RÃ¤umen
- Sofortalarm bei ungewÃ¶hnlicher TÃ¼rÃ¶ffnung oder Manipulation
- Kopplung von Zutrittsprotokoll mit Live-Ã?berwachung (z.â?¯B. Alarm auf Smartphone/Pager)

4. Sensibilisierung des technischen Personals

- Schulung zu TÃ¤terverhalten und sozialen Manipulationstechniken
- EinfÃ¼hrung einer Eskalationsregel: â??Lieber einmal zu viel stoppen als einmal zu wenig.â??
- Standardisierte Ã?bergabeprozesse und RÃ¼ckmeldungen bei Dienstende

Fazit: Der TÃ¤ter nutzte keine LÃ¼cke im GebÃ¤ude â?? sondern im Denken

Â© www.security-explorer.de

Der Vorfall mit dem falschen Techniker war kein Zufall â?? sondern das logische Ergebnis eines Systems, in dem **Vertrauen, Gewohnheit und fehlende Schulung** gefÃ¤hrliche Allianzen eingehen.

Wo keine Sicherheitskultur herrscht, genÃ¼gt eine einfache TÃ¤uschung, um kritische Systeme zu kompromittieren.

Mit dem KRITIS-Dachgesetz gibt es keine Ausrede mehr fÃ¼r fehlende Prozesse. Kliniken tragen Verantwortung â?? fÃ¼r Menschenleben, Versorgungssicherheit und BetriebskontinuitÃ¤t. Und diese beginnt nicht an der Schranke, sondern **im Inneren der Organisation â?? beim Denken, Handeln und Entscheiden jedes Einzelnen.**

Quellenangaben
Titelbild von HNFOTO â?? stock.adobe.com

Â© Security Explorer