

## HOHER SCHUTZ VOR VIREN UND PHISHINGMAILS

Im Basler Claraspital nimmt die Informationssicherheit einen zentralen Stellenwert ein. Die first frame networkers wurden damit beauftragt, das Netzwerk des Spitals vor den zunehmenden Cyberrisiken bestmöglich zu schützen.



### Der Kunde

Das Claraspital in Basel ist ein privat geführtes Akutspital und ein unverzichtbarer Teil der Gesundheitsversorgung in der Nordwestschweiz. Es zeichnet sich durch hervorragende Behandlungen, umfassende medizinische Kompetenzen und den Betreuungsstandard eines Privatspitals aus. Das Claraspital führt zwei Zentren – das Bauchzentrum und das Tumorzentrum –, ist Referenzspital für Adipositas und betreibt die Spezialitäten Innere Medizin/Endokrinologie, Pneumologie, Urologie, Kardiologie sowie Gynäkologie/Gynäkologische Onkologie. Das bedeutendste rechtsrheinische Akutspital leistet überdies eine erweiterte Grundversorgung mit einem 24-Stunden-Notfall und Ambulatorien. Insgesamt beschäftigt das Claraspital, das in diesem Jahr seinen 90. Geburtstag feiert, rund 1200 Mitarbeitende.

### Die Ausgangslage

Im Gesundheitswesen ist Informationssicherheit zentral, so auch im Claraspital. Um die in diesem Bereich sehr hochgesteckten Ziele zu erreichen, werden organisatorische sowie technische Hilfsmittel benötigt. Da die Bedrohung durch Viren und Malware, die von den üblichen signaturbasierten Antivirenlösungen nicht mehr erkannt werden (z. B. Verschlüsselungstrojaner), stetig steigt, suchte das Claraspital nach einer passenden Lösung für diese Herausforderung.

### Der Nutzen für den Kunden

Mit einer Sandbox-Lösung werden Dateien oder Links auf virtuellen Systemen geöffnet und deren Verhalten und Änderungen am System durch einen intelligenten Algorithmus analysiert. Stellt die Sandbox fest, dass die geöffnete Datei diverse verdächtige Modifikationen vornimmt, wird sie als Schadsoftware klassifiziert. Durch den Einsatz dieser Technologie konnte der Schutz vor Viren und Phishingmails im Claraspital deutlich erhöht werden.

### Umsetzung:

Die eingesetzten Produkte und Services sind von Fortinet, dem führenden Anbieter für IT-Sicherheitslösungen.

**FORTINET**

«Wir sind schon lange sehr zufrieden mit den first frame networkers. Auch stellten wir fest, dass die Betreuung von Netzwerk und Security aus einer Hand für uns absolut Sinn macht.»

Matthias Klinke, Leiter IT-Infrastruktur-Management  
St. Claraspital AG, Basel



**Herr Klinke, Sie haben sich für den Einsatz einer Sandbox zur Optimierung der IT-Sicherheit entschieden. Was war der Auslöser?**

Auslöser waren die zunehmende Bedrohung durch Ransomware und die immer gezielteren Angriffe auf das Gesundheitswesen. Früher bot ein klassischer Virenschutz noch ausreichend Schutz vor den meist primitiven Mails mit Schadsoftware. Dies hat sich allerdings in den letzten Jahren stark verändert. Heute laufen die Attacken immer öfter sehr gezielt ab. So hatten wir schon seriös scheinende Bewerbungen, deren Anhang ein Worddokument mit Macro enthielt, das eine Ransomware laden wollte.

**Was gab bei Ihrer Wahl einer Fortinet-Lösung den Ausschlag?**

Wir sind schon seit längerer Zeit sehr zufrieden mit den first frame networkers, die bis anhin «nur» unsere LAN- und WLAN-Infrastruktur betreuten. Als ein Firewallwechsel anstand, haben wir uns deshalb an die first frame networkers gewandt, die unser Anliegen dann mit einem FortiGate-Cluster bestens umsetzten. Die Bedienung ist für uns einfach und übersichtlich. Ausserdem konnten wir schnell feststellen, dass die Betreuung von Netzwerk und Firewall aus einer Hand für uns absolut Sinn macht.

**Wie lief das Projekt für Sie als Auftraggeber ab?**

Die first frame networkers hängten eine Sandbox als POC (proof of concept) ins Netzwerk. Als wir nach wenigen Tagen in das Log der Sandbox sahen, entdeckten wir, dass diese sehr gut arbeitete. Es wurden etliche Mails blockiert, deren angehängte URLs nicht sauber waren. Meist sollte über einen Link Schadsoftware heruntergeladen werden. Innert weniger Wochen konnten wir so viele URLs mit der Sandbox blocken. Heute arbeiten bei uns im Netzwerk Firewall, Mail-Gateway und Sandbox Hand in Hand zusammen. Ich bin froh über die von den first frame networkers vorgeschlagene Lösung.

**Sind Sie mit der Unterstützung durch die first frame networkers ag zufrieden?**

Wir haben mit den first frame networkers einen Partner gefunden, der uns in den Bereichen Netzwerk und Security sehr viel Arbeit abnimmt. Das Claraspital ist zu klein, um ein eigenes Team mit Spezialisten aufbauen zu können, die ein so tiefes Fachwissen besitzen wie die first frame networkers. Deshalb ist es für uns ideal, einen so kompetenten und verantwortungsbewussten Partner an unserer Seite zu haben.

**stClaraspital**  
In besten Händen.

first frame networkers ag  
haldenstrasse 1  
ch-6340 baar  
[www.firstframe.net](http://www.firstframe.net)  
[info@firstframe.net](mailto:info@firstframe.net)  
+41 41 768 08 00