SWS
COMPUTERSYSTEME
Member of ACP Group

# HACKER Ziel No.1: KRANKENHÄUSER

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verzeichnet seit einiger Zeit eine Zunahme von Cyberangriffen auf Krankenhäuser sowie Medizin-Firmen.

IT for innovators.

Member of ACP Group

# Krankenhäuser in der Coronakrise Ziel von Hacker-Angriffen

## Herausforderung:

Es kursieren beispielsweise E-Mails zu neuen Corona Studien mit einem Link zu einem Preprint-Server, auf dem die Ergebnisse einsehbar sind.
Immer öfter werden offizielle Stellen wie die WHO Weltgesundheitsorganisation als Absender missbraucht, um Schadsoftware zu platzieren. Neue Domainnamen mit dem Begriff „Corona" sind exorbitant gestiegen. Viele davon mit dem Ziel User zu verleiten die Website zu besuchen und Informationen preiszugeben.

Leider reicht oftmals der Besuch einer Website schon aus, um sich unbemerkt zu infizieren. Sollten Kollegen von Ihnen im Home-Office arbeiten und eventuell sogar private Endgeräte (Smartphone und Tablet eingeschlossen) nutzen, sind Sicherheitslücken oftmals um ein vielfaches höher.

## Lösung:

SWS DNS Security. Die DNS Security Lösung von SWS ist ein cloudbasierter Dienst, der Sie immer und überall auf der Welt schützt. Schatten-IT wird sichtbar und Sicherheitslücken, die durch diese Applikationen entstehen, können Sie schnell und unkompliziert eindämmen.
Das Ausrollen der Lösung in Ihrer Organisation ist kinderleicht und im „Handumdrehen" erledigt. Mit Hilfe der SWS DNS Security erhalten Sie eine detaillierte Auswertung zu den Angriffsversuchen mit allen relevanten Zahlen, Daten und Fakten .

## Unser Angebot für Sie:

Für Interessenten gibt es derzeit Lizenzen, die wir kostenlos zur Verfügung stellen. Die Lizenzen sind auf User-Basis und völlig frei skalierbar. Danach sind diese Lizenzen monatlich kündbar und es besteht keine Mindestvertragslaufzeit. Kommen Sie gerne auf uns zu, wir helfen Ihnen natürlich bei der Einrichtung.

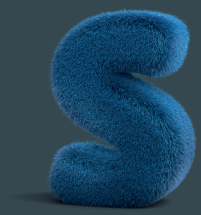
## Ihr Nutzen

- Filter für mehr Inhaltskategorien
- Schutz der Benutzer
- Echtzeit-Aktivitätssuche
- Kundenspezifisches Black- und Whitelisting
- Risikobewertung
- Identifikation gezielter Angriffe

**Sie möchten mehr über DNS Security erfahren?**
So erreichen Sie uns:

SWS Computersysteme AG
+49 8586 9604 0
vertrieb@sws.de

# SWS Experten Tipps
## Einfach für Sie da!



**Vorsicht bei E-Mails, die vorgeben von der WHO oder anderen offiziellen Stellen zu stammen:**
Nutzer sollten direkt auf deren Websites gehen, um die neuesten Informationen zu erhalten. Generell sollten keine Links in E-Mails von unbekannten Absendern angeklickt werden.

**Umgehend melden:**
Alle bösartigen E-Mails und Angriffe sollten direkt an die IT-Abteilungen zur Untersuchung und Behebung gemeldet werden.

**Keine Informationen preisgeben:**
Nutzer sollten niemals persönliche Informationen oder Anmeldedaten auf eine E-Mail-Anfrage preisgeben. Auf diese Weise kann ein Phishing-Angriff zu einem BECAngriff (Business-E-Mail Compromise) führen.

**E-Mails von unternehmensinternen Stellen:**
Nutzer sollten zudem besonders wachsam bei E-Mails von internen Abteilungen oder Führungskräften sein, die innerhalb des Unternehmens augenscheinlich über den Coronavirus-Ausbruch informieren. Domain- und Anzeigenamen-Spoofing sind einige der beliebtesten Techniken von Cyberkriminellen.

**Security-Technologien:**
Unternehmen sollten sicherstellen, dass sie über einen zuverlässigen Viren-, Malware- und Anti-Phishing-Schutz verfügen.

**Mitarbeiterschulung:**
Darüber hinaus sollten alle Mitarbeiter eine aktuelle Schulung über die neuesten Phishing- und Social-Engineering-Angriffe erhalten.

**Sie möchten mehr über DNS Security erfahren?**
So erreichen Sie uns:

SWS Computersysteme AG
+49 8586 9604 0
vertrieb@sws.de

www.sws.de