SUCCESS STORY

FROM THE COLLABORATION

sure[secure]
your security operations center

BIG
direkt gesund

Introduction

Bundesinnungskrankenkasse Gesundheit is a German guild health insurance fund based in Berlin with administrative offices in Dortmund. BIG direkt gesund is open nationwide and has branches in Dortmund, Düsseldorf, Cologne and Aachen.

With 520,000 policyholders, BIG direkt is ranked 29th out of 103 statutory health insurers in Germany.

As a health insurance company, BIG is an important building block for citizens and is therefore regarded as a critical infrastructure for Germany.

BIG
direkt gesund

Federal Guild Health Insurance Health

Industry:	Finance & Insurance
Employees:	1.000
Founded:	1996
Insured:	520.000

These topics are part of the success story

- Detection via Managed Detection & Response Service
- Incident Response Management
- Security Operations Center as a Service
- Cyberinsurance

What challenges did the partner face?

The Bundesinnungskrankenkasse Gesundheit (BIG) has fallen victim to a cyber attack.

A group of attackers succeeded in compromising the system landscape. The attack was discovered by a service provider with whom BIG has a Managed Detection & Response contract. The service provider was able to detect the attacker before any encryption or data outflow occurred, but systems had to be shut down proactively or preventively.

At the beginning, it was difficult to assess the extent of the attack due to a lack of visibility. As no Security Information and Event Management (SIEM) had been implemented at the time to analyse the logs centrally, analysing the incident took a lot of time.

At the same time, the existing cyber insurance was massively increased in price by the insurer and even cancelled after the security incident. This situation illustrates a contradiction: despite increased security measures, insurers often react with price increases or cancellations because they see an increased risk.

This is because a cyber attack usually results in significantly stronger cyber security. The knowledge gained leads to important measures being implemented, which improves cyber resilience.

If this background is discussed in detail with the insurer, it can even lead to better insurability and optimised conditions. With a well-founded analysis and a clear road map, a specialised broker can negotiate successfully with insurers.

Good relationships with insurers and a detailed presentation of security measures increase the chances of obtaining suitable insurance cover.

How did we solve the challenge?

We realised very quickly what we would need in this case:

- Incident Response Team
- Transparency & visibility
- Efficient processes and intensive support

Incident Response

After suresecure's analysts detected the first anomalies during the night, the partner was informed that an attacker probably had access to the environment. Together with BIG's IT technicians, further investigations were carried out and the theory was ultimately confirmed. To prevent further damage, the servers were proactively disconnected from the network and the internet connection was blocked.

Our forensics teams scanned all systems and checked them in particular for the identified Indicators of Compromise (IOCs). As a result, every infected system had to be proactively reinstalled. Our Security Operations Centre Service (SOC Service) was also rolled out to increase visibility within the infrastructure. This enabled us to ensure that all logs from all assets were collected and analysed centrally. Should the attacker manage to remain persistent in the environment despite our efforts, we at least have total visibility and therefore the ability to react very quickly to the events. At the same time, we supported the partner with crisis communication and discussions with the authorities and insurance companies.

Cyberinsurance

The cyber insurance was cancelled by the insurer while the lawsuit was still ongoing and the premium was massively increased. This was initially accepted so as not to jeopardise the payment of monetary damages. Twelve months later, the insurer cancelled the policy again and changed the conditions. As a result, it was no longer economically viable to continue the insurance. Clear signals were also sent that the insurance company had no interest in paying for the damage.

BIG had very little time to look for alternatives due to the cancellation of the insurance at short notice and therefore asked us for support. In addition, it is not so easy for KRITIS companies to obtain insurance, as the potential for damage is higher. It is also not so easy to obtain insurance after a loss has occurred. It is necessary to demonstrate to insurers that adequate measures have been taken.

I have been involved in many security incidents, but this one was special. Mainly because the impact on the insured was so great and it was simply a matter of being able to provide benefits again as quickly as possible.

But especially because of the noticeably cooperative partnership with all the contacts at BIG. That was really great cinema.

Baran Kamaci
Enterprise Account Executive
suresecure GmbH

Today's setup

Today, all logs are sent to suresecure's Security Operations Centre and we are able to intervene much earlier should another attack occur, as we now receive all logs compared to an MDR service. The SOC service is also a strategic tool with regard to the implementation law of the NIS2 directive. This imposes new requirements on KRITIS companies like BIG in particular, which BIG already fulfils.

Reports from the SOC are made available to the insurance company on a monthly basis. However, these are not simply sent out, but also discussed with the insurance company.

DWe discuss the quantity and quality of the alerts, talk about possible escalations and the current threat situation and provide a transparent overview of vulnerability management. This gives the insurer a very good feeling for the risk assessment.

This is because, among other things, improvement measures are also mapped, which in turn can lead to better premiums and conditions. The transparency also increases the insurer's willingness to pay in the event of a claim. This is because the reports mean that the insurer cannot say afterwards: ‘We didn't realise that’.

I love solving puzzles. This one was particularly tricky and demanded a lot from all of us. Everyone involved in this project has grown and I am very grateful for the experience I was able to gain on this project.

André Ditzel
Senior IR-Analyst
suresecure GmbH

Andreas Faltin, IT Manager BIG Direkt

We work together with suresecure to increase our level of security at a strategic and conceptual level as well as in the operational implementation of security issues. We are impressed by the high level of commitment, professionalism and sense of responsibility of the suresecure team. This enables a very pleasant, goal-orientated collaboration based on a high level of trust, even in difficult situations.

Key Take-Aways:

- 🟩 Early detection is extremely important, to minimise consequential damage
- 🟩 Visibility and transparency in the own infrastructure create full ability to act
- 🟩 Cyber insurance can also be taken out despite cyber attack and KRITIS affiliation

In our podcast, Michael Döhmen talks to exciting guests about cybersecurity topics every 14 days.

suresecure Gmbh
Dreischeibenhaus 1
40211 Düsseldorf

Phone: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.eu