

“Transparency Pays Off”

What to Do in the Event of a Cyberattack? A Communications Expert from Mainz Offers Advice.

The number of cyberattacks is steadily rising. Data theft, crippled point-of-sale systems and communication channels, and halted production lines—anything is possible. For companies, the question is not so much whether they will be attacked, but when—says Matthias Goldbeck, a Mainz-based partner at the Strategic Communication Consultant Network [CCounselors GmbH & Co. KG].

Since the onset of the COVID-19 pandemic, when working from home and video conferencing suddenly boomed, this trend has become even more pronounced. Goldbeck’s basic rule can also be derived from the pandemic: Preparation does not protect against an attack, but it often prevents severe consequences. This involves both IT security and behavioral guidelines—as well as communication. According to Goldbeck, what to do in the event of a successful cyberattack should be a topic for the executive board—as well as for the entire organization and the supervisory board. Risk management systems without cybersecurity? That is no longer acceptable. The expert advises putting together interdisciplinary crisis teams comprising IT, legal, financial, communications, production, and logistics specialists, provided the company has a sufficiently broad organizational structure.

“Business leaders should critically and without reservation consider what could happen in the worst-case scenario and draw up plans for this worst-case scenario so they don’t have to start from scratch,” says Goldbeck. This also includes determining in which areas external consulting should be sought—whether in communications or from specialized cybersecurity providers, some of whom also conduct negotiations on behalf of companies with cybercriminals. “It’s best to secure such specialists in advance.” It is important to simulate scenarios and prepare talking points. Training sessions with experts who have already gained practical experience with attacks are the most effective.

Putting up a wall to the outside world is not a solution. For Goldbeck, communication—both internal and external—is key, alongside the technical aspects of defense and problem-solving: “Communication belongs at the decision-making table from the very beginning.”

Goldbeck considers keeping things under wraps out of concern that the company’s reputation will suffer from having been attacked to be misguided: “You are the victim here, not the perpetrator. That’s how it is in the public eye, too. You run into problems when you sweep things under the rug and fail to adequately inform customers and employees. Transparency is rewarded. No one wants to be accused of failing to give customers and employees the opportunity to protect themselves.”

Of course, you should only communicate what has already been confirmed. And there are legal obligations regarding what must be reported to data protection authorities and when. “Informing people when data is at risk is, for me, a cardinal virtue,” says Goldbeck. “The clock starts ticking the moment the attack is detected.” It is important to keep an eye on how the company is being reported on and discussed—for example, on social media. “Whoever manages to get ahead of the wave retains control over the narrative.” It is also essential that employees know how they’re allowed to speak publicly and privately: “Everyone needs the essential facts and must know what they can and are allowed to say.”

It is quite possible that, in the event of an attack, the usual communication channels will no longer function. Communication without email, phone and video conferencing systems, or the intranet? Even in this scenario, operational capability and the dissemination of information must be ensured through alternative structures—such as messaging apps and personal email addresses, which, ideally, are available offline.

As Goldbeck emphasizes, all companies are well advised to train their staff on IT security: do not open unknown attachments or suspicious emails, and do not click on links that are not definitively trustworthy. The user is usually the target of the attack. Criminals’ most popular business model right now is to steal data and hold it hostage. Anyone who does not want their data to end up on the dark web must pay a ransom in cryptocurrency.

These scenarios must also be carefully considered. Which data is critical, and what concessions is one willing to make? “You should be clear in advance about how to respond to potential demands,” says Goldbeck. After all, the better prepared—and thus more confident—the victim is in crisis management, the less damage will result.

12 Rules for Effective Crisis Communication

1. Plan for the unexpected
2. Practice, practice, practice
3. Communication is a core discipline
4. The principles of crisis communication apply
5. Monitor the situation to act quickly and “master” social media
6. Establish alternative communication structures
7. Internal communication is key
8. Communicate actively and transparently with the outside world
9. An attack must not come as a surprise

10. The topic should be on the agenda regularly
11. Access rights as a potential risk area
12. Ensure sufficient capacity and expertise

Torben Schröder, freelance journalist

Translated from the article “Transparenz wird honoriert”, Report 02/2025 – Wirtschaftsmagazin der Region Rheinhessen, IHK für Rheinhessen. Original article (German) on ihk.de