AIRNITE

ZERO DAY

ISSUE 18/2026 · IT SECURITY

Black October: two German administrations in emergency mode – and what companies can learn

In October 2026, cyberattacks hit the town of Eichstätt and the district of Oberspreewald-Lausitz in Germany. Servers encrypted, around 1.4 terabytes of data copied, weeks without email or vehicle registration. What happened and what every organisation can take from it.

Published: 21 November 2026 Reading time: 6 min Author: Airnite editorial team

SOFTWARE. SECURITY. CODE.

// THE SITUATION IN NUMBERS

≈ 1.4 TB
data copied in Eichstätt
about a quarter of the data, presumably including personal data (Town of Eichstätt)

≈ 1,000
systems checked in the OSL district
servers and notebooks (Oberspreewald-Lausitz district)

20 Oct–9 Nov
no email with the district administration
Oberspreewald-Lausitz district

Supplier
way in at Eichstätt
flaw in a vendor's software, despite two-factor authentication (Town of Eichstätt)

Two administrations, two German states, one month: in October 2026, the **town of Eichstätt** in Bavaria and the **district of Oberspreewald-Lausitz** in Brandenburg had to switch to emergency mode after cyberattacks. Both kept the public informed on their own websites – and thus show very concretely what such an attack means in everyday life.

// What happened?

In **Eichstätt**, according to the town, a ransomware attack began on the night of 8 to 9 October; in a later announcement, the town names 8 October as the day of intrusion. Servers were encrypted. On 3 November, the town announced that the perpetrators had copied around **1.4 terabytes** of data, about a quarter of its entire data, presumably including personal data – such as master data from applications, registration, tax and bank data. According to the town, there was no explicit ransom demand. The town now reports that the town hall is offering all services again.

In the **Oberspreewald-Lausitz district**, no email exchange with the district administration was possible from the evening of 20 October. Around **1,000 systems**, including servers and notebooks, were checked. Vehicle registration was down. Only on 9 November was the district reconnected to the state administration network and email working again; digital registration resumed on 12 November, the driving licence office on 13 November. According to the district, it initially remained open whether data had been stolen.

// How does the attack work?

Eichstätt has disclosed the attackers' route: they came in through a **security flaw in the software of a vendor** the town worked with – despite two-factor authentication. According to the town, there were no signs of phishing, and it was not a targeted attack on the administration. The town cut off the vendor's access and no longer intends to work with it.

The approach is typical of today's ransomware: copy data, then encrypt, then threaten publication. Eichstätt rebuilt its servers from the latest backups after an integrity check; the backups were stored on several servers in German data centres. The Oberspreewald-Lausitz district shut down its systems and checked them one by one before bringing them back online.

// Who is affected?

Citizens were affected first: no email contact, no vehicle registration, limited appointments. In Eichstätt, there is the added issue that personal data may have fallen into the wrong hands; the town notified the Bavarian data protection commissioner.

Both cases are instructive for companies. Entry via a service provider, weeks-long outages of central services and the question of which data was stolen apply to every company just the same. Size hardly matters: anyone with reachable systems and service provider access can be hit.

// What should you do now?

The key lessons: remote access by service providers is a favourite way in and needs its own controls. Backups must be stored separately, and restoration must be rehearsed. And open, regular communication – as both administrations practised with their own information pages – helps maintain trust. The checklist below sums up the steps.

// How does Airnite help?

In **consulting**, Airnite works with you on an emergency and recovery plan and reviews your service providers' access. With **penetration tests**, we show where an attacker would get in today. In **training**, we prepare administrations and staff for an emergency – including communication.

> Note: the information comes from the information pages of the town of Eichstätt and the Oberspreewald-Lausitz district; some of the town's dates differ slightly. Research status: 21 November 2026.

Checklist: what to do now

[+] Record all remote access by software vendors and service providers, secure it and enable it only when needed.

[+] Keep backups separate from the production network and regularly rehearse restoring entire servers.

[+] Define which services must come back first in an emergency (e.g. email, specialist applications, telephony).

[+] Prepare emergency communication: status page, phone announcements, contact channels for citizens, customers and staff.

[+] Know your data protection duties: notify the supervisory authority within 72 hours and inform those affected where required.

[+] Communicate openly after the incident – regular updates build trust.

How Airnite helps

- Consulting – An outside view of your plans and projects.
- Penetration Testing & Security – Controlled attacks with a clear report and action plan.
- Training – Your team learns our tools and processes.

How quickly would you be operational again after an attack?

Airnite reviews service provider remote access, backups and emergency plans with you – from an attacker's perspective and with the goal of a fast recovery. For municipalities and companies alike: clear, prioritised and without scaremongering.

Request an initial call · Send an email · Via WhatsApp

Contact

Questions about this article? Message us on WhatsApp: +49 174 6834842

Read online: https://airnite.de/en/magazine/municipalities-cyberattack-october-2026-emergency/

Sources

Every fact in this article is based on the sources below. Primary sources are marked.

1. **Town of Eichstätt · Cyberattack (announcements and information)** · 22 Oct 2026 to 18 Nov 2026 · PRIMARY SOURCE
   Primary source: start of the attack, way in, encrypted servers, amount of copied data, recovery
   https://www.eichstaett.de/cyberangriff/
2. **Stadt Eichstätt · Cyber-Attacke: Hacker/-innen erbeuteten rund 1,4 Terabyte Daten** · 3 Nov 2026 · PRIMARY SOURCE
   Primary source: 1.4 TB copied, data categories affected, notification of the data protection commissioner
   https://www.eichstaett.de/aktuelles/cyber-attacke_hacker-innen_erb-2883/
3. **Landkreis Oberspreewald-Lausitz · IT-Sicherheitsvorfall im Landkreis OSL** · 21 Oct 2026 to 13 Nov 2026 · PRIMARY SOURCE
   Primary source: shutdown, around 1,000 systems, email outage, vehicle registration, reconnection
   https://www.osl-online.de/news/1/1300878/nachrichten/it-sicherheitsvorfall-im-landkreis-osl.html

General editorial information, not legal advice and not an assessment of your individual systems. Status: date of publication.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de