EACG
Enterprise Architecture Consulting Group

SECURITY DIALOGUES
No. 10 · 9 October 2026
Marcus Hale (PSIRT) · Tess Calder (red team) · Nora Voss (guest) · Jessy Lang

Now It's Yours

Seven things to get right when you run the platform yourself, and how to choose

A self-hosted vulnerability platform held every known weakness in the company, 14 months out of date, with an install-day admin account, reachable from every office subnet. Nothing was wrong with the product. They ran it as if it were nobody's system. Run it properly, or hand it to somebody who will. The only wrong answer is yes by default.

BORROWED TRUST
Relying on a vendor's practice without having chosen to.

1. Can you find it?

2. Do you know who owns it?

3. Do you know its version?

THE HONEST TEST FOR RUNNING IT YOURSELF

1	**A named owner and a deputy** Projects end, and what they installed does not.	Name a person, not a team alias, with calendar entries behind the name: a monthly update window, a standing path for emergency fixes, a quarterly restore test. A few hours a month. Name a deputy too.
2	**A tested update path** An untested upgrade fails on the day it matters.	Rehearse on a copy, on a boring afternoon. Update the software monthly, and test the upgrade before it goes live.
3	**A tested restore** A backup you have never restored is a rumour.	Restore last night's backup onto a staging copy, then run the next update against it. Same afternoon, while nothing depends on the answer.
4	**Narrow, watched admin access** Install-day credentials and shared logins.	Single sign-on with a second factor. Roles that match jobs. Service accounts scoped to what they scan. One break-glass admin account, kept offline and alarmed. Access logs read by a person, on a calendar.
5	**A network position that fits** The map sits next to the territory it describes.	Give it a management zone of its own: own segment, own admin accounts, not the production domain's. Reachable from a handful of places, not every subnet. Treat it as tier one.
6	**Encryption, keys elsewhere** A locked door with the key taped to it.	Encrypt in transit and at rest, in the database and the backups. Disk encryption alone only stops a stolen disk. Keep the key wrapped by another key held elsewhere, run by different people. Rehearse rotating it.
7	**Hearing about fixes the same day** Publishing a fix is not the fleet running it.	Subscribe to the vendor's channel on day one, with a name next to the subscription, and make sure someone reads it. Ask: how fast, and what does applying it cost in downtime and revalidation?

CHOOSING ON PURPOSE: THREE QUESTIONS

Is there a hard constraint?
Data that may not leave, a network with no route out, a contract or regulator that says so. If yes, the decision is made: do it well, or find a professional who runs it inside your constraint.

Can you name the capacity?
A fraction of a person, and a calendar. A name on a calendar is the test, good intentions are not. If you cannot name it, hosted is the better deal.

What do you borrow, what do you assume?
For each hosted tool, write down what you borrow: patching, monitoring, backup, access control, incident response. Ask the vendor to confirm it in writing.

Listen to the episode
Now It's Yours and the rest of the series.
eacg.de
/en/podcast/s10-borrowed-trust

Digital Product Design
From the first idea to a viable first release.
eacg.de
/en/consulting/digital-products

PSIRT Services
Intake, assess and disclose vulnerabilities, built or run as a service.
eacg.de
/en/consulting/psirt

© 2026 EACG GmbH