Connecting Software

case study

Preventing Sensitive Data Exposure in SharePoint: Lessons from a German Agricultural Association

| MASCHINENRINGE SUCCESS STORY

“[CB Dynamics 365 to SharePoint Permissions Replicator] is a silent worker in the background who does its job and nothing else. It doesn’t suddenly pop up or cause problems. It does what it should do!”

LEANDER KIRNER,
TEAM LEAD CRM & REPORTING AT MASCHINENRINGE

Customer
Maschinenringe

Activity
Agricultural services

Country
Germany

Product Application
CB Dynamics 365 to SharePoint Permissions Replicator

When internal innovation introduces external risk, how quickly and smartly you respond can define your long-term security posture.

That's exactly what happened at Maschinenringe, a leading German agricultural association, when they identified a potential risk with their new internal social intranet application. The app connected users to SharePoint documents that were supposed to be accessible only through Dynamics 365, which could mean sensitive internal content was at risk of exposure—until Maschinenringe made a decisive move to close the gap.

Let's break down what happened, how they solved it, and what your organization can learn from their approach.

The Vulnerability: SharePoint as a Potential Open Backdoor

Maschinenringe had followed all Microsoft recommendations when setting up the integration between Dynamics 365 and SharePoint. They had decided that employees would access documents through Dynamics only, so that the access rules defined in Dynamics would be enforced and only users with the necessary permissions would be able to access sensitive files.

But a new intranet app changed the rules.

By connecting directly to SharePoint, this app would give employees access to document libraries they were never supposed to see. And because SharePoint permissions are not automatically synced with Dynamics roles, the gates would effectively be open to all SharePoint users.

This was simply not an option as Leander Kirner, Team Lead CRM & Reporting at Maschinenringe explained. "***There was a lot of sensitive data and documents,***" he said.

This scenario is not uncommon. Many organizations rely on the default Dynamics-to-SharePoint integration, assuming permissions will carry over as both systems are Microsoft, and the integration itself is Microsoft. They don't. Without a solution to bridge that permissions gap, companies risk unintentional data leakage, especially when other platforms tap into SharePoint content directly.

The Results: Security Without Overhead

The results speak for themselves:

- No unauthorized SharePoint file access

- No need for manual permission handling
- No support tickets over a full year of operation

Kirner calls the solution a ***"silent worker in the background"***—one that does its job without creating noise, delays, or distractions.

That's the kind of automation most IT teams dream about.

Key Takeaways for IT Leaders

1. **Assume nothing is secure by default.**

Microsoft's integration between Dynamics and SharePoint doesn't include permission alignment. Maschinenringe resolved this permissions gap before it became an issue. Follow their lead: never rely solely on default settings; always verify your security configurations end-to-end.

2. Plan for the ripple effect of new tools.

A potential vulnerability emerged at Maschinenringe with the introduction of a new internal application, but it was identified and addressed before it became an issue. This highlights the importance of regularly reviewing your security model when new systems are integrated.

3. Automate before it becomes urgent.

Maschinenringe acted before a breach occurred. This type of forward-thinking decision saved them from both regulatory risk and internal disruption.

Want to See How It Works?

If your Dynamics is integrated with SharePoint or any new platforms are entering your environment, Maschinenringe's experience should raise one big question:

Are your permissions still aligned?

CB Dynamics 365 to SharePoint Permissions Replicator

Let's Talk

Connecting Software

THANK YOU

1776 S Jackson St, Suite 602
Denver, CO 80210
United States
Phone: +1 (720)-577-3030

Handelskai 340/5
1020 Vienna,
Austria
Phone: +43 1 3707 200

Poľná 5626
901 01 Malacky
Slovakia
Phone: +421 (0) 34 7725637

Rua João de Deus, 12 E - Fr. C
9050-027 Funchal
Madeira Island - Portugal
Phone: (+351) 291 945 098

Microsoft Partner
Gold DevOps
Gold Data Analytics
Gold Data Platform
Gold Application Development
Gold Windows and Devices

Windows Server 2019 Certified

Microsoft Azure Certified

Microsoft Azure Government

salesforce PARTNER SINCE 2019

TÜV SÜD

TÜV SÜD

2021 INNOVATION INDEX

CONNECTING-SOFTWARE.COM

OFFICE@CONNECTING-SOFTWARE.COM