

# Sure, Let Business Users Build Their Own. What Could Go Wrong?

Michael Bargury @ Zenity  
BSidesLV 2023

# Hi there 🖐️

- CTO and Co-founder @ Zenity
- OWASP LCNC Top 10 project lead
- Dark Reading columnist
- Defcon, BSides, RSAC, OWASP
- Hiring top researchers, engs & pms!



@mbrg0



[github.com/mbrg](https://github.com/mbrg)



[darkreading.com/author/michael-bargury](https://darkreading.com/author/michael-bargury)



# Agenda

1. Business users are building their own
2. What could go wrong?
3. How can we fix it?

# Enterprise LCNC – EVERYONE is a Developer

# Business Needs



## IT Capacity



Sure, Let Business Users Build Their Own.  
What Could Go Wrong?

@mbrg0  
BSideLV 2023

Power Apps | App

Search

Environment  
PowerAddicts (default)

Back

+

Insert

Add data

...

Editing

Fill

=

fx

White

Tree view

ScreensComponents

Search

+ New screen

> App

Screen1

SCREEN

Add an item from the Insert pane or connect to data

Screen1

50 %

Copilot

PREVIEW

What do you want to do?

Describe what you want to do with this app, and AI will do it for you.

Add a text labelAdd a galleryAdd a buttonAdd an email screen

What do you want to do with this app?

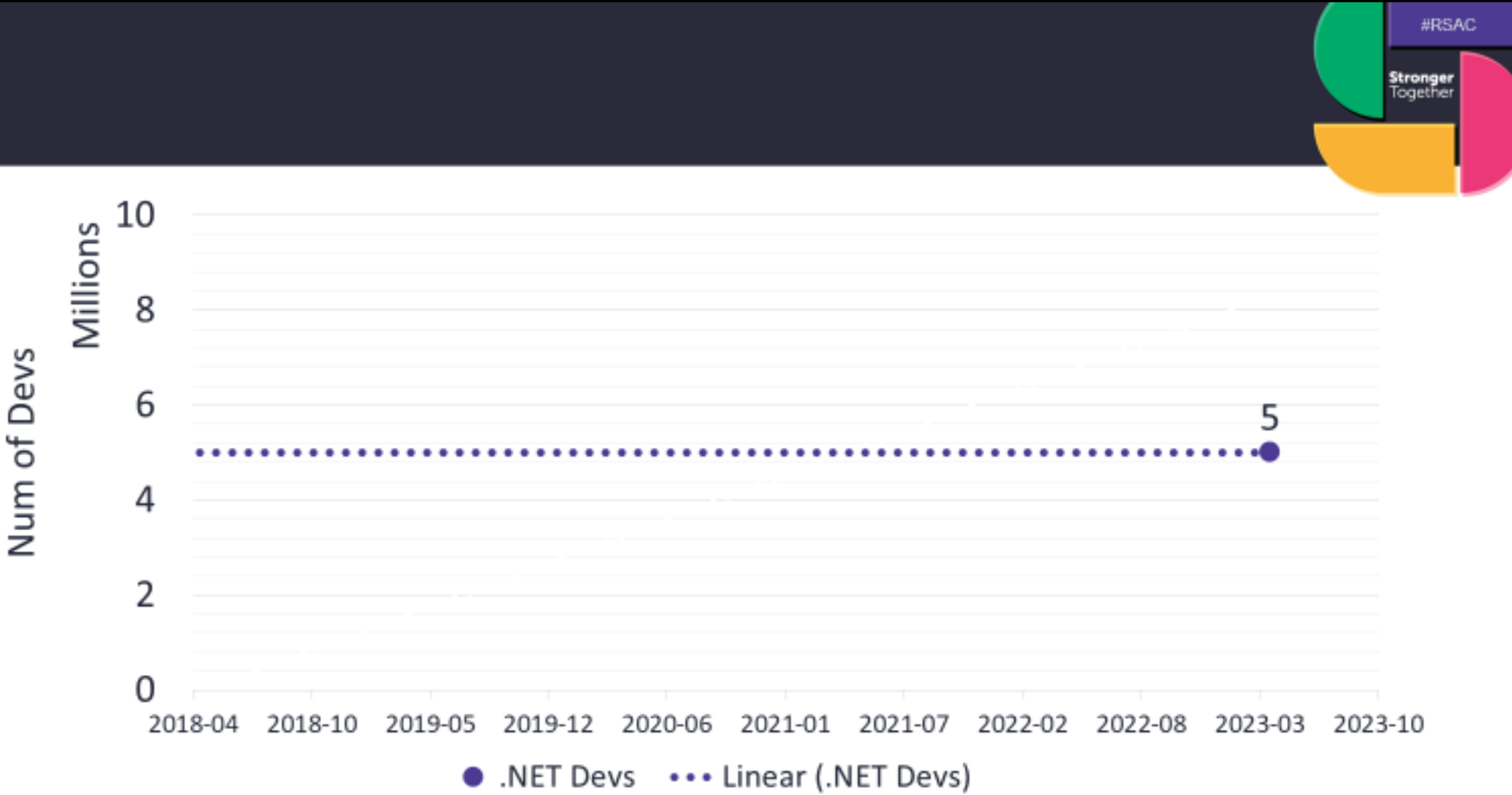
Make sure AI-generated content is accurate and appropriate before using. [See terms](#)

Source:  
@RezaDorrani

@mbrg0  
#BHUSA@BlackHatEvents



# Is this actually being used?



Sources: Microsoft Build 2018, Ignite 2019, Build 2020, Protocol 2022

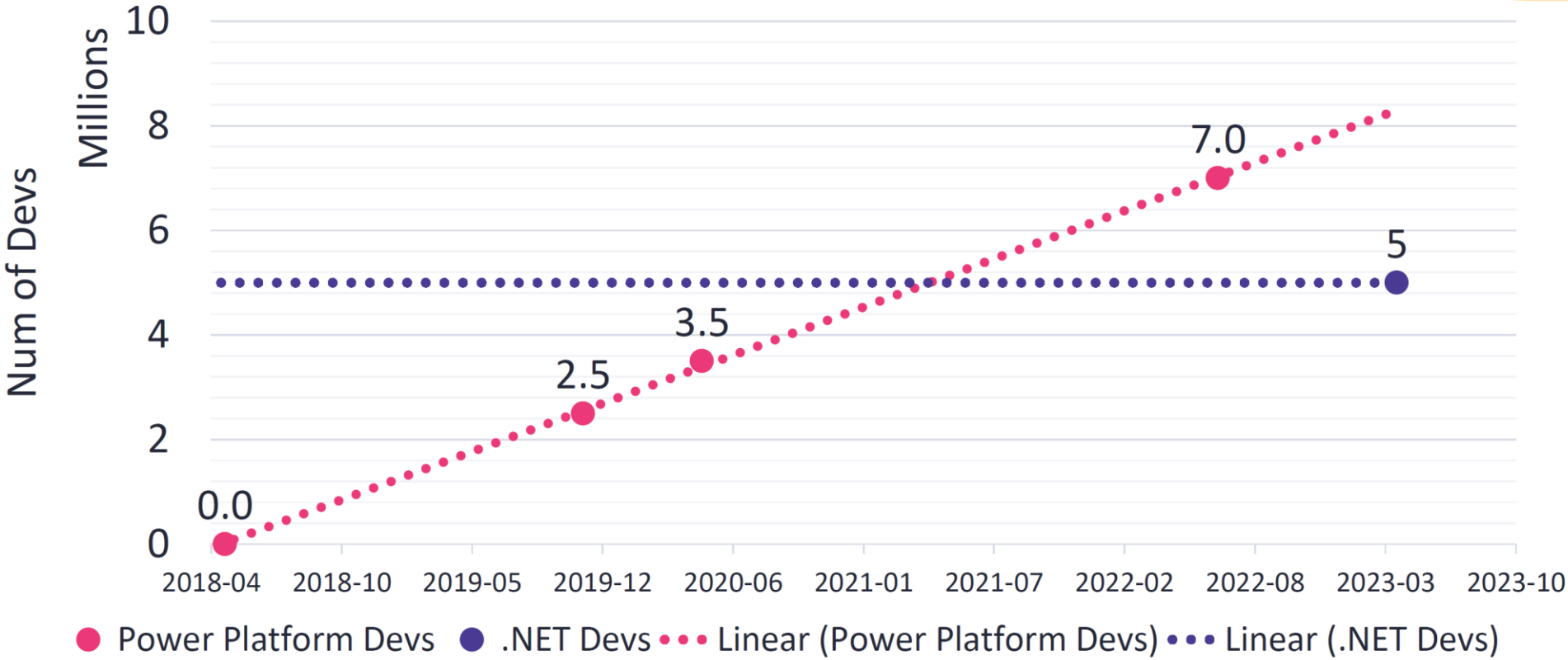


*Credential  
Sharing as a  
Service: The Dark  
Side of No Code*

Michael Bargury  
RSAC 2023

~8M active Power devs today!

More MSFT low-code devs than .NET devs, today!



Sources: Microsoft Build 2018, Ignite 2019, Build 2020, Protocol 2022

Credential  
Sharing as a  
Service: The Dark  
Side of No Code

Michael Bargury  
RSAC 2023





# What could go wrong?

# OWASP LCNC Top 10

- LCNC-SEC-01: Account Impersonation
- LCNC-SEC-02: Authorization Misuse
- LCNC-SEC-03: Data Leakage and Unexpected Consequences
- LCNC-SEC-04: Authentication and Secure Communication Failures
- LCNC-SEC-05: Security Misconfiguration
- LCNC-SEC-06: Injection Handling Failures
- LCNC-SEC-07: Vulnerable and Untrusted Components
- LCNC-SEC-08: Data and Secret Handling Failures
- LCNC-SEC-09: Asset Management Failures
- LCNC-SEC-10: Security Logging and Monitoring Failures



# Real-world stories

# Story #1 – employee onboarding

Power Apps

Home

Create

Learn

Apps

Tables

Connections

Solutions

Flows

More

Power Platform

Ask a virtual agent

Search

Environment  
Zenity Stage (default)

AA

Start from

Blank app

Create an app from scratch and then add your data

Watch video

Dataverse

Start from a Dataverse table to create a three-screen app

Watch video

SharePoint

Start from a SharePoint list to create a three-screen app

Watch video

Excel

Start from an Excel file to create a three-screen app

Watch video

SQL

Start from a SQL data source to create a three-screen-app

Watch video

Image

Upload an image of an app and we'll convert it into an app


Watch video

## Start from



## Blank app

Create an app from scratch and then add your data

 Watch video



## Dataverse


## Start from a Dataverse table to create a three-screen app

 [Watch video](#)



## SharePoint

## Start from a SharePoint list to create a three-screen app

 [Watch video](#)



## Excel

Start from an Excel file to create a three-screen app




## SQL

Start from a SQL data source to  
create a three-screen-app



Image

Upload an image of an app icon :   
and we'll convert it into an app



Power Apps | Employee Onboarding

Search

Back

+

Insert

Add data

...

Editing

Fill

=

fx

White

Tree view

Screens

Components

Search

+ New screen

> App

Screen1

Label2\_4

TextInput1\_5

Textinput\_1

LblAppName3\_1

IconAccept1\_1

IconCancel1\_1

Label2\_3

Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number

Save

SCREEN

Screen1

Properties

Advanced

Ideas

Fill

Background image

None

Image position

Fit

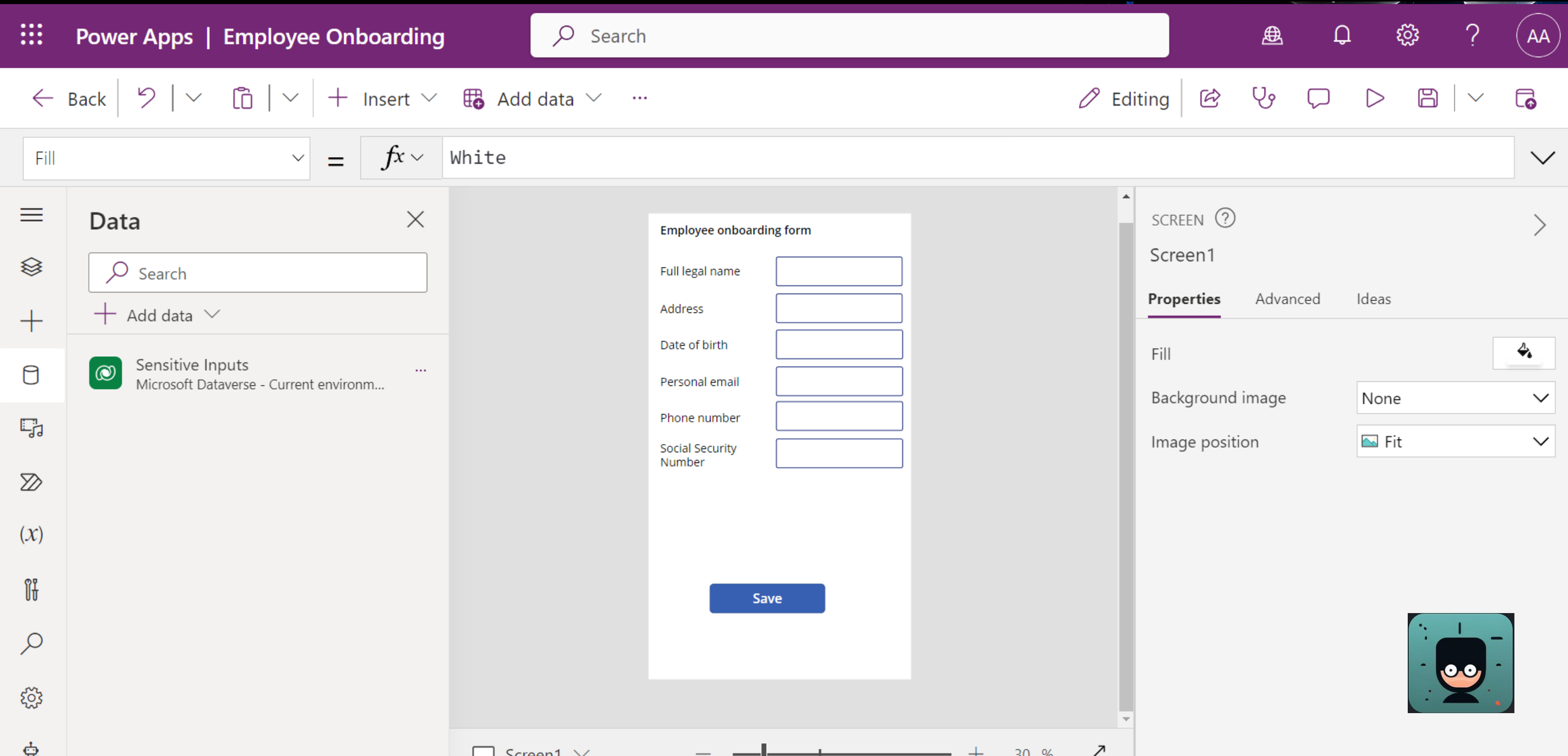
Screen1

30 %



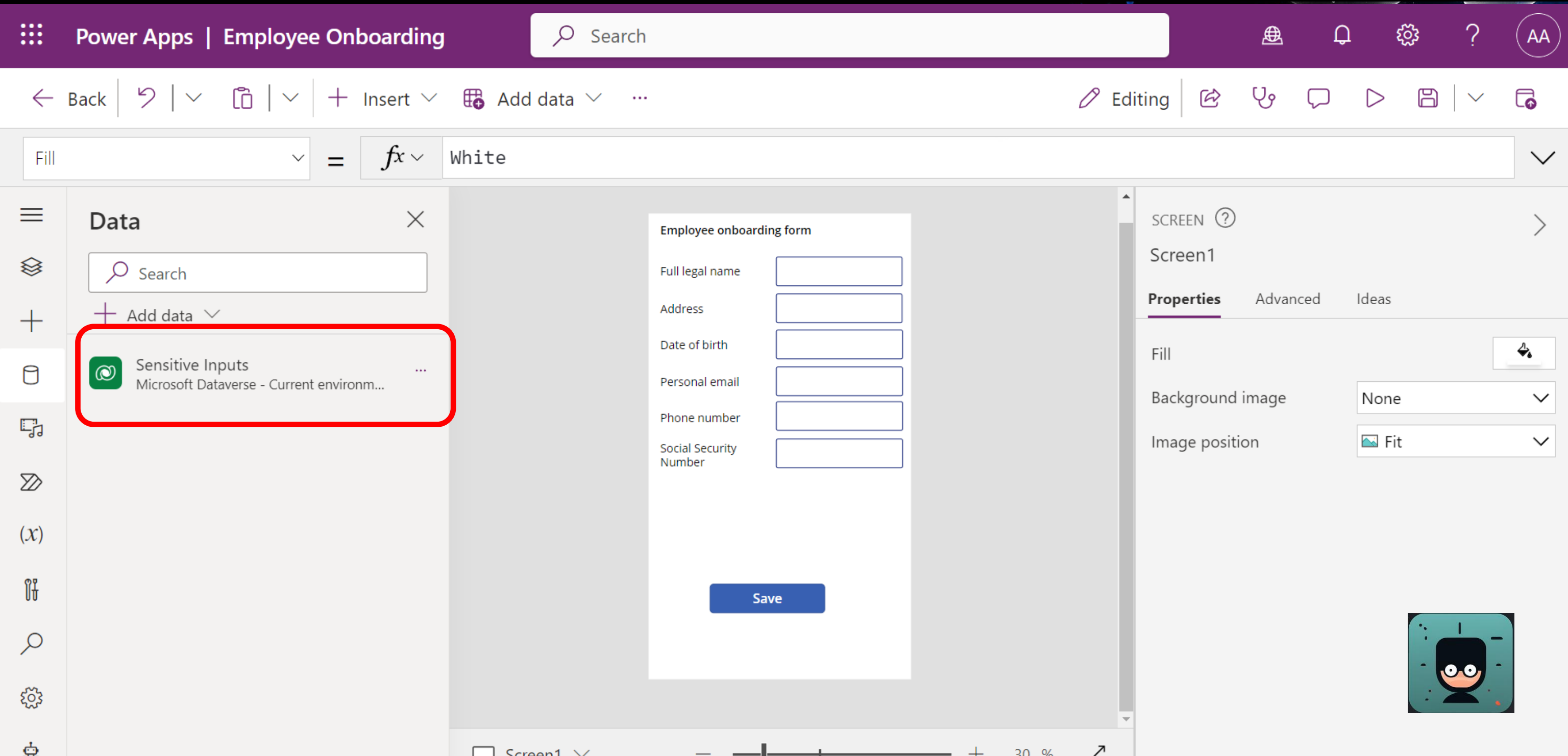
## What could go wrong:

@mbrg0  
BSideLV 2023



## What could go wrong:

@mbrg0  
BSideLV 2023



The diagram illustrates the Microsoft Power Platform architecture. At the top, the Microsoft Power Platform logo is displayed, followed by the text: "The low code platform that spans Microsoft 365, Azure, Dynamics 365, and standalone apps." Below this, five main components are shown in a row: Power BI (Business analytics), Power Apps (App development), Power Automate (Process automation), Power Virtual Agents (Intelligent virtual agents), and Power Pages (External-facing websites). These components are connected to a central hub labeled "Data connectors". Below the Data connectors, three additional components are shown: AI Builder, Dataverse, and a user profile icon.

## What could go wrong:

@mbrg0  
BSideLV 2023

The screenshot displays the Power Automate interface for a flow named "Update Employee Info in HR system". The flow is composed of two steps:

- When a row is added, modified or deleted**: This is the trigger step, which is connected to the second step.
- Send email (V2)**: This is the action step, which is expanded to show its configuration.
  - To**: hrorg@cloudcore.com
  - Subject**: New Employee Update info
  - Body**: The body is configured with a rich text editor. It includes a list of data fields: SSN, Contact, Email, Address, and Employee Name. The fields are displayed as a list of items, each with a small icon and a close button (x).
  - Attachments**: There are three fields for attachments:
    - Attachments Name - 1**: Title of the attachment.
    - Attachments Content - 1**: Body of the attachment.
    - Attachments Content-Type - 1**: Type of content in the attachment.
  - + Add new item**: A button to add more attachment items.

At the bottom of the flow canvas, there are two buttons: **+ New step** and **Save**.

# Employee onboarding – findings



Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number

Save

<

<



Power Apps

Search

Environment  
Zenity Stage (default)

KS

+

New table 

▼

↶

Import 

▼

↷

Export 

▼

Search

Tables

Recommended

Custom

All

Table <div>↑</div> <div>▼</div>	Name <div>▼</div>	Type <div>▼</div>	Managed <div>▼</div>	Customizable <div>▼</div>	Tags <div>▼</div>
Account	account	Standard	Yes	Yes	Core
Address	customeraddress	Standard	Yes	Yes	Standard
AppFlow Relation	cr6e4_appflowrel...	Standard	No	Yes	Custom
Appointment	appointment	Activity	Yes	Yes	Productivit
asjs	cr6e4_asjs	Standard	No	Yes	
Attachment	activitymimeatta...	Standard	Yes	Yes	

Home

Create

Learn

Apps

Tables

Connections

Solutions

Flows

More

Power Platform

Ask a virtual agent





Sure, Let Business Users Build Their Own.  
What Could Go Wrong?

@mbrgO  
BSideLV 2023

Power Apps

Search

Environment

Zenity Stage (default)

KS

Home

Create

Learn

Apps

Tables

Connections

Solutions

Flows

More

Power Platform

Ask a virtual agent

New table

Open

Edit

Import

Export

Properties

Search

	Position		position	Standard	Yes	Yes	System
	Query		cr6e4_querytest	Standard	No	Yes	Custom
	Recurring Appointment		recurringappoint...	Activity	Yes	Yes	Standard
	res		cr6e4_res	Standard	No	Yes	Custom
✓	Sensitive Input		cr6e4_sensitivein...	Standard	No	Yes	Custom
	table_for_app_with_im...		cr6e4_table_for_...	Standard	No	Yes	Custom
	Task		task	Activity	Yes	Yes	Productivit
	Team		team	Standard	Yes	Yes	System
	Team template		teamtemplate	Standard	Yes	Yes	
	ttr		cr6e4_ttr	Standard	No	Yes	
	User		systemuser	Standard	Yes	Yes	Standard

Power Apps

Search

Environment  
Zenity Stage (default)

KS

← Back

+ New row

∨

+ New column

↺ Refresh

🧩 Create an app

✎ Edit table properties

⚡ Update forms and views

Abc

📊 Sensitive Inputs ✎

Data saved

	Employee Name * ↑ ∨	SSN ∨	Address ∨	Contact ∨	+19 more ∨	+
	Jamie Reading	209-97-1111	jamier@zenitydemo.OnMicrosoft....			
	Brooklyn Gonzalez	209-97-9876	brooklynd@zenitydemo.OnMicros...			
	Henry Mitchell	209-97-0987	henryd@zenitydemo.OnMicrosoft...			
	Savannah Perez	209-97-7890	savannahp@zenitydemo.OnMicro...			
	Ella Gonzalez	209-97-9876	ellaq@zenitydemo.OnMicrosoft.c...			
	Riley Mitchell	209-97-0987	rileyp@zenitydemo.OnMicrosoft.c...			
	Nathan Perez	209-97-7890	nathanh@zenitydemo.OnMicroso...			
	Daniel Martin	209-97-6789	danielm@zenitydemo.OnMicrosof...			
	Layla Gonzalez	209-97-9876	laylam@zenitydemo.OnMicrosoft			

# Employee onboarding – findings

- Data accessible to all (Authorization Misuse)



# Employee onboarding – findings

- Data accessible to all (Authorization Misuse)
- Sensitive data in plain text (Data and Secret Handling Failures)



Power Apps | Employee Onboarding

Environment  
Zenity Stage (default)

ZH

Employee onboarding form

Full legal name

Daniel Wood

Address

New York 3rd street

Date of birth

11 Jan 1990

Personal email

Danielw124@gmail.com

Phone number

202-555-0117

Social Security Number

78-05-1120

Save



## What could go wrong:

@mbrg0  
BSideLV 2023

Power Automate

Search

Environments  
Zenity Stage (default)

?

ZH

← Update Employee Info in HR system

Undo Redo Comments Save Flow checker Test

When a row is added, modified or deleted

Send email (V2)

To

hrorg@cloudcore.com

Subject

New Employee Update info

Body

Font 12 B I U

SSN x

Contact x

Email x

Address x

Employee Name x

Attachments Name - 1

Title of the attachment.

Attachments Content - 1

Body of the attachment.

Attachments Content-Type - 1

Type of content in the attachment.

+ Add new item

Show advanced options

+ New step

Save

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Ask a chatbot

Sure, Let Business Users Build Their Own.  
What Could Go Wrong?

@mbrgO  
BSideLV 2023

Power Automate

Search

Environments

Zenith Stage (default)

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Ask a chatbot

Update Employee Info in HR system • Ran at 8/7/2023 7:40:51 PM

Your flow ran successfully.

When a row is added, modified or deleted

INPUTS

Show raw input

Change type

4

Table name

cr6e4\_sensitiveinput

Scope

4

OUTPUTS

Show raw output

body

"cr6e4\_name": "Daniel Wood",

"\_modifiedby\_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",

"\_modifiedby\_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemusers",

"\_modifiedby\_type": "systemusers",

"cr6e4\_ssn": "78051120",

"createdon": "2023-08-07T16:40:48Z",

"ItemInternalId": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",

"SdkMessage": "Create"

Connection: zivh@zenithstage.com

When a row is added, modified or deleted

When a row is added, modified or deleted

"headers": {

"Expect": "100-continue",

"Host": "prod-52.westeurope.logic.azure.com",

"x-ms-correlation-request-id": "d7b3daa4-0bba-4724-918b-4523e1bb2e75",

"x-ms-client-request-id": "d7b3daa4-0bba-4724-918b-4523e1bb2e75",

"x-ms-user-id": "7cb2f429-a54a-46c3-8e4f-df3a3032f249",

"Content-Length": "1258",

"Content-Type": "application/json"

}

body": {

"cr6e4\_email": "daniel1ds@gmail.com",

"\_owningbusinessunit\_value": "edfdf52a-e501-ec11-94ee-0022488000bc",

"\_owningbusinessunit\_value@Microsoft.Dynamics.CRM.lookuplogicalname": "businessunits",

"\_owningbusinessunit\_type": "businessunits",

"statecode": 0,

"\_statecode\_label": "Active",

"cr6e4\_sensitiveinputid": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",

"statuscode": 1,

"\_statuscode\_label": "Active",

"cr6e4\_contact": "202-555-0117",

"\_createdby\_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",

"\_createdby\_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",

"\_createdby\_type": "systemusers",

"cr6e4\_dateofbirth": "10.10.1990",

"\_ownerid\_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",

"\_ownerid\_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",

"\_ownerid\_type": "systemusers",

"modifiedon": "2023-08-07T16:40:48Z",

"cr6e4\_address": "116 E 60TH ST NEW YORK USA",

"cr6e4\_name": "Daniel Wood",

"\_modifiedby\_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",

"\_modifiedby\_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",

"\_modifiedby\_type": "systemusers",

"cr6e4\_ssn": "78051120",

"createdon": "2023-08-07T16:40:48Z",

"ItemInternalId": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",

"SdkMessage": "Create",

"RunAsSystemUserId": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7"

}



Sure, Let Business Users Build Their Own.  
What Could Go Wrong?

@mbrgO  
BSideLV 2023

Power Automate

Search

Environments  
Zenity Stage (default)

?

ZH

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Update Employee Info in HR system

Edit

Owners

Adding an owner gives them full control of this flow, so make sure you only share with people you trust. They'll be able to add or remove other users as owners, access the run history, and can update, edit or delete this flow.  
[Learn more](#)

Add a user or group as owner

Enter names, emails, or user groups

Ziv Hagbi

HR-Ali

Embedded connections

Everyone listed as an owner will have access to all these connections and will only be able to use them in this flow.  
[Learn more](#)

Connections in use

Connections listed are actively being used in this flow. [Manage connections](#)


zivh@zenitystage.com

Microsoft Dataverse

maortzury@gmail.com

Gmail

Ask a chatbot



# Employee onboarding – findings

- Data accessible to all (Authorization Misuse)
- Sensitive data in plain text (Data and Secret Handling Failures)
- Sensitive data written to logs (Data Leakage)

```
"body": {  
  "cr6e4_email": "daniel1ds@gmail.com",  
  "_owningbusinessunit_value": "edfdf52a-e501-ec11-94ee-0022488300bc",  
  "_owningbusinessunit_value@Microsoft.Dynamics.CRM.lookuplogicalname": "bu",  
  "_owningbusinessunit_type": "businessunits",  
  "statecode": 0,  
  "_statecode_label": "Active",  
  "cr6e4_sensitiveinputid": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",  
  "statuscode": 1,  
  "_statuscode_label": "Active",  
  "cr6e4_contact": "202-555-0117",  
  "_createdby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",  
  "_createdby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",  
  "_createdby_type": "systemusers",  
  "cr6e4_dateofbirth": "10.10.1990",  
  "_ownerid_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",  
  "_ownerid_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",  
  "_ownerid_type": "systemusers",  
  "modifiedon": "2023-08-07T16:40:48Z",  
  "cr6e4_address": "116 E 60TH ST NEW YORK USA",  
  "cr6e4_name": "Daniel Wood",  
  "_modifiedby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",  
  "_modifiedby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",  
  "_modifiedby_type": "systemusers",  
  "cr6e4_ssn": "78051120",  
  "createdon": "2023-08-07T16:40:48Z",  
  "ItemInternalId": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",  
  "SdkMessage": "Create",  
  "RunAsSystemUserId": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",  
  "RowVersion": "12774383"  
}
```

# Employee onboarding – findings

- Data accessible to all (Authorization Misuse)
- Sensitive data in plain text (Data and Secret Handling Failures)
- Sensitive data written to logs (Data Leakage)

# Story #2 – productivity sync

⋮

Power Automate

🔍 Search

🌐 Environments

Zenity Stage (default)

⚙️ ?

KS

☰

Home

Approvals

**My flows**

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

← Sync Outlook to Gmail

↶ Undo

↷ Redo

💬 Comments

💾 Save

🔗 Flow checker

🧪 Test

📧

When a new email arrives (V3)

?

⋮

↓

✉️

Send email (V2)

?

⋮

\* To

KS

Kris Smith

×

Subject

📧

Subject

×

Body

Font

▼

12

▼

**B**

*I*

U

🖋️

☰

⋮

☰

☰

🔗

🔗

</>

📧

Body

×

Attachments

📧

Attachments

×

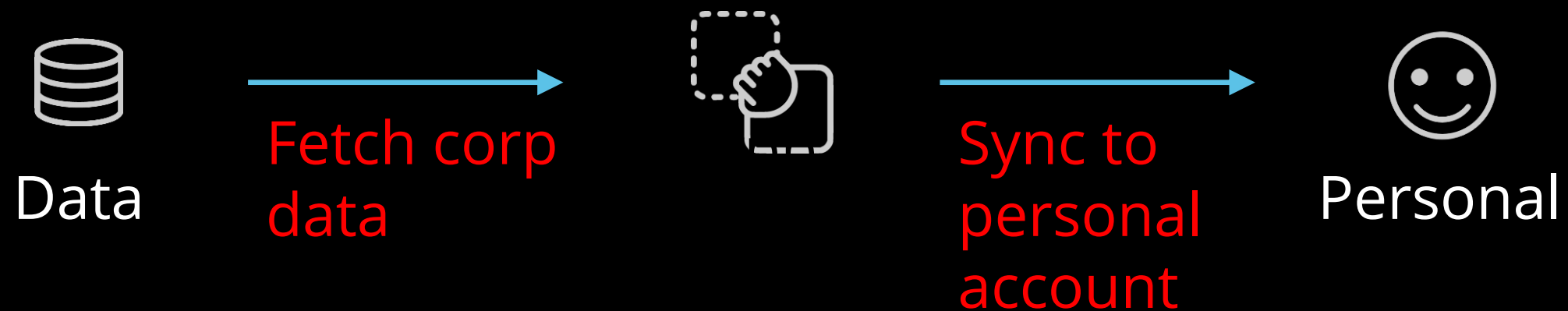
📎

👤

# Productivity sync – findings

# Productivity sync – findings

- Business data to personal account (Data Leakage)





Sure, Let Business Users Build Their Own.  
What Could Go Wrong?

@mbrgO  
BSideLV 2023

Power Apps | Set up your email sync

Environment  
Zenity Stage (default)

KS

Back | Undo | Redo | Insert | Open Sans | 15 | Semibold | ...

Editing | Share | Help | Run | Save | ...

OnSelect =  $\text{fx}$  SyncOutlookhistorytoGmail.Run(NumberInput,EmailInput)

Power Automate

Search

Add flow

In your app

Sync Outlook history to Gmail

SyncOutlookhistorytoGmail

Sync Outlook history to Gmail

Email address

Text input

How many emails to sync

Sync your email

Button ?

Button1

Properties | **Advanced** | Ideas

Search for a property ...

ACTION

OnSelect

SyncOutlookhistorytoGmail.Run  
(NumberInput,EmailInput)

DATA

Text

"Sync your email"

Tooltip

" "



## Sync Outlook history to Gmail

Email address

How many emails to sync

Sync your email





Power Apps

Search

Home

Create

Learn

Apps

Tables

Flows

Chatbots

AI models

Solutions

Cards

Choices

Connections

Dataflows

More

Edit

Play

Share

Apps > Set up your email sync

Details

Versions

Connections

Owner

Kris Smith

Description

Not provided

Created

8/8/2023, 1:34:51 AM


Modified

8/8/2023, 1:34:51 AM

Web link

<https://apps.powerapps.com/p/5594523476b3&sourcetime=2>

Mobile QR code



every

EC

Everyone in CloudCore

KS

Kris Smith  
Owner

Share Set up your email sync

Add people as Users and Co-owners to your app. Make sure your data connections have been shared with all users.

Email message

Let colleagues know what your app does and how it can help them.


Include an image

Add an image to the email to showcase what your app looks like.  
Tip: Use an image that is 4:3 aspect ratio and smaller than 1MB.

Choose a file to upload or drag and drop it here.

Upload

Select or add a user to set their permissions



Power Apps

Search

Home

Create

Learn

Apps

Tables

Flows

Chatbots

AI models

Solutions

Cards

Choices

Connections

Dataflows

More

Edit

Play

Share

Apps > Set up your email sync

Details

Versions

Connections

Owner

Kris Smith

Description

Not provided

Created

8/8/2023, 1:34:51 AM


Modified

8/8/2023, 1:34:51 AM

Web link

<https://apps.powerapps.com/p/5594523476b3&sourcetime=2>

Mobile QR code



Share Set up your email sync

Add people as Users and Co-owners to your app. Make sure your data connections have been shared with all users.

Enter a name, email address, or Everyone

New users

EC

Everyone in CloudCore

User

Shared with

Sort by Name

KS

Kris Smith

Owner

Choose a file to upload or drag and drop it here.

Upload

Everyone in CloudCore

Everyone can use this app.

An organization can't edit or share apps.

☐ Co-owner

Can use, edit, share app but not delete or change owner.

Data permissions

Make sure your users have access to the data used in your app, including gateways, APIs, connectors, and tables.

Logic flows

Office 365 Outlook

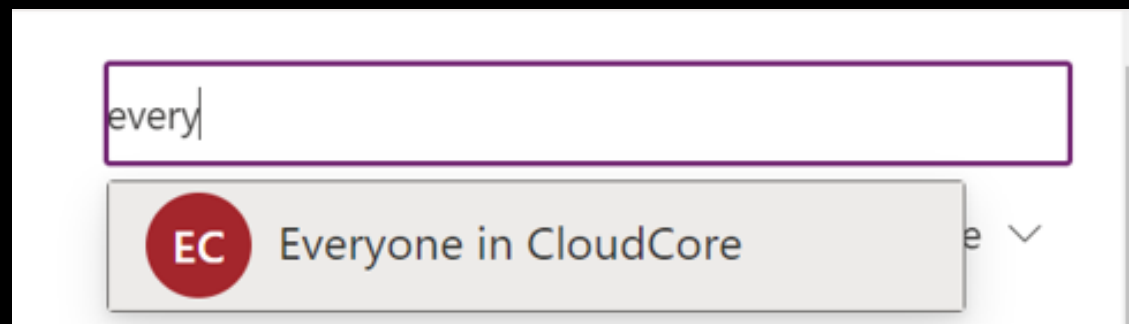
Gmail

Send an email invitation to new users

# Productivity sync – findings

- Data Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)

Everyone means  
**EVERYONE**, including  
guests by-default

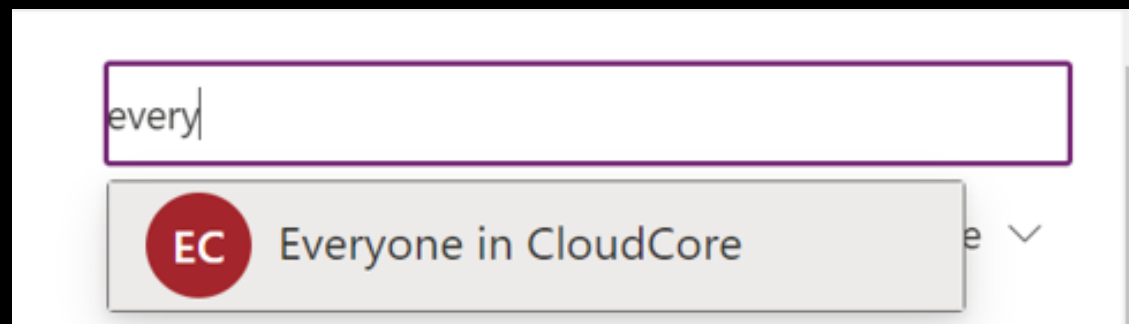


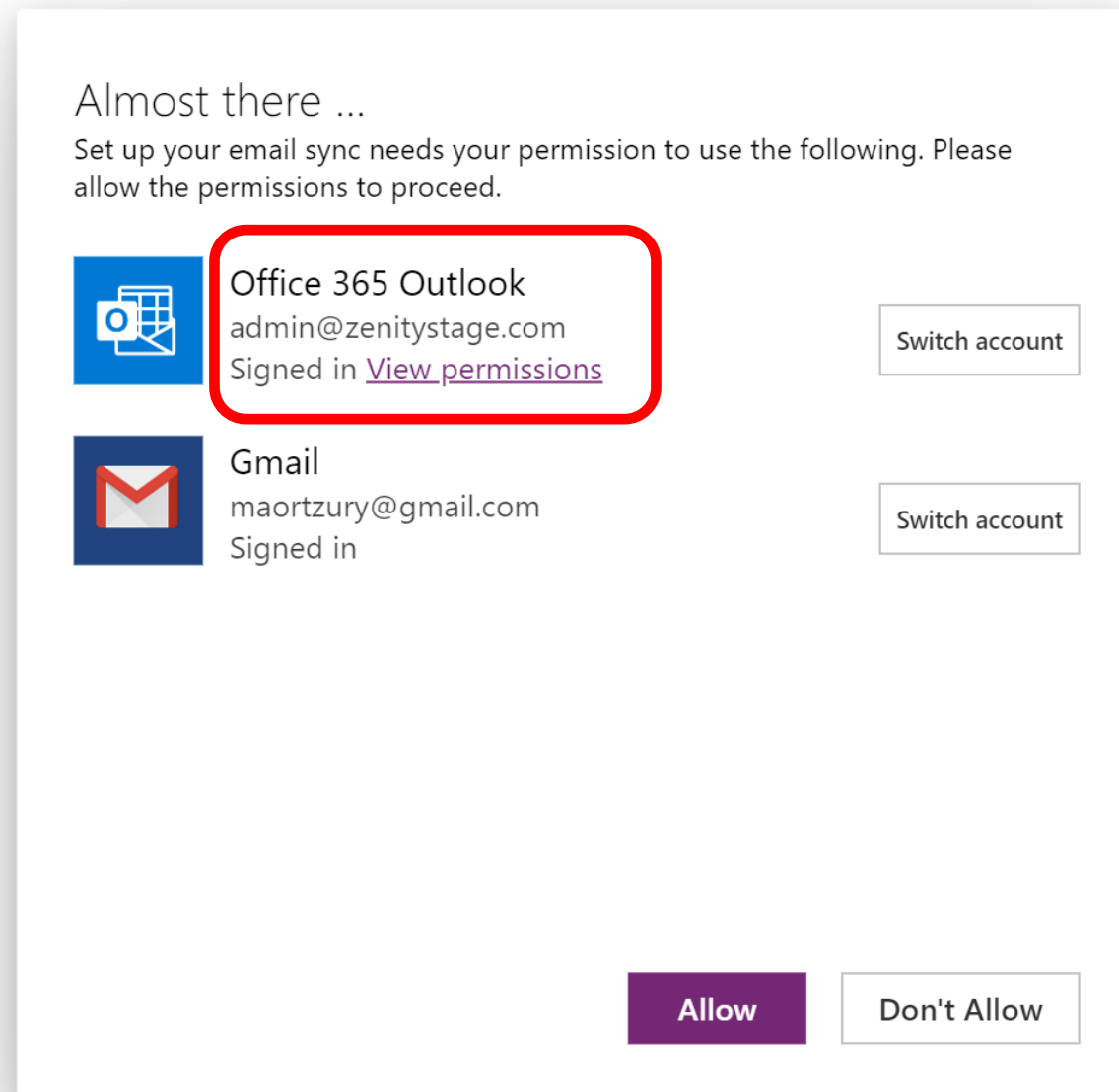
## Productivity sync – findings

- Data Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)

Everyone means  
EVERYONE, including  
guests by-default

Check out the talk ***All You Need Is Guest*** for an  
attacker's perspective!







## Sync Outlook history to Gmail

Email address

How many emails to sync

Sync your email



Power Automate

Search

Environments  
Zenity Stage (default)

Settings

Help

KS

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Sync Outlook history to Gmail • Ran at 8/8/2023 1:48:09 AM

Resubmit Cancel Edit Help

PowerApps (V2)0s

↓

Get last X emails with attachments2s

↓

For each email32s

Power Automate

Search

Environments  
Zenity Stage (default)

Settings

Help

KS

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Sync Outlook history to Gmail • Ran at 8/8/2023 1:48:09 AM

Resubmit Cancel Edit

For each email

5s

Previous Previous failed Show 1 of 5 Next failed Next

Send email to myself

1s

INPUTS

Show raw inputs

To

imkrissmith@gmail.com

Subject

Admin Admin1 has shared the Weekly Timesheet app with you

Body

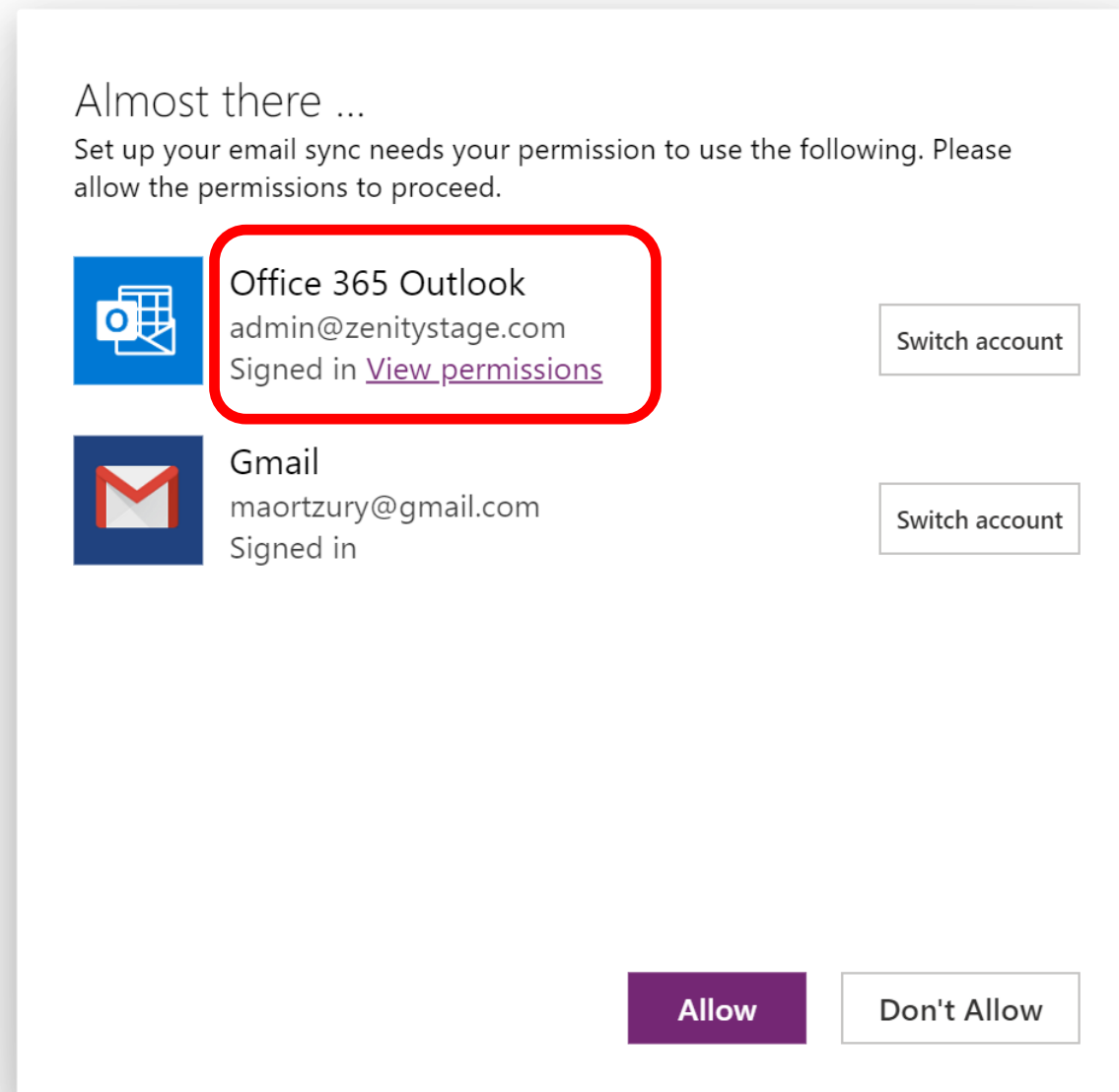
<p><html lang="en" style="min-height:100%; background:#ffffff"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><!--@media only screen and (max-width: 640px) {wrap-dangler



# Productivity sync – findings

- Data Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)
- Personal data leaks to logs (Data Leakage)





# Phishing made easy

Can we fool users to create connections for us?

- Set up a bait app that does something useful
- Generate connections on-the-fly
- Fool users to use it
- Pwn their connection (i.e. account)

☒ Account takeover

***Low Code High Risk:  
Enterprise Domination via  
Low Code Abuse***

Michael Bargury  
DEFCON 30

Check out [power-pwn](#)  
on GitHub!

## Productivity sync – findings

- Data Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)
- Personal data leaks to logs (Data Leakage)

Sure, Let Business Users Build Their Own.  
What Could Go Wrong?

@mbrg0  
BSideLV 2023



# Story #3 – self-service

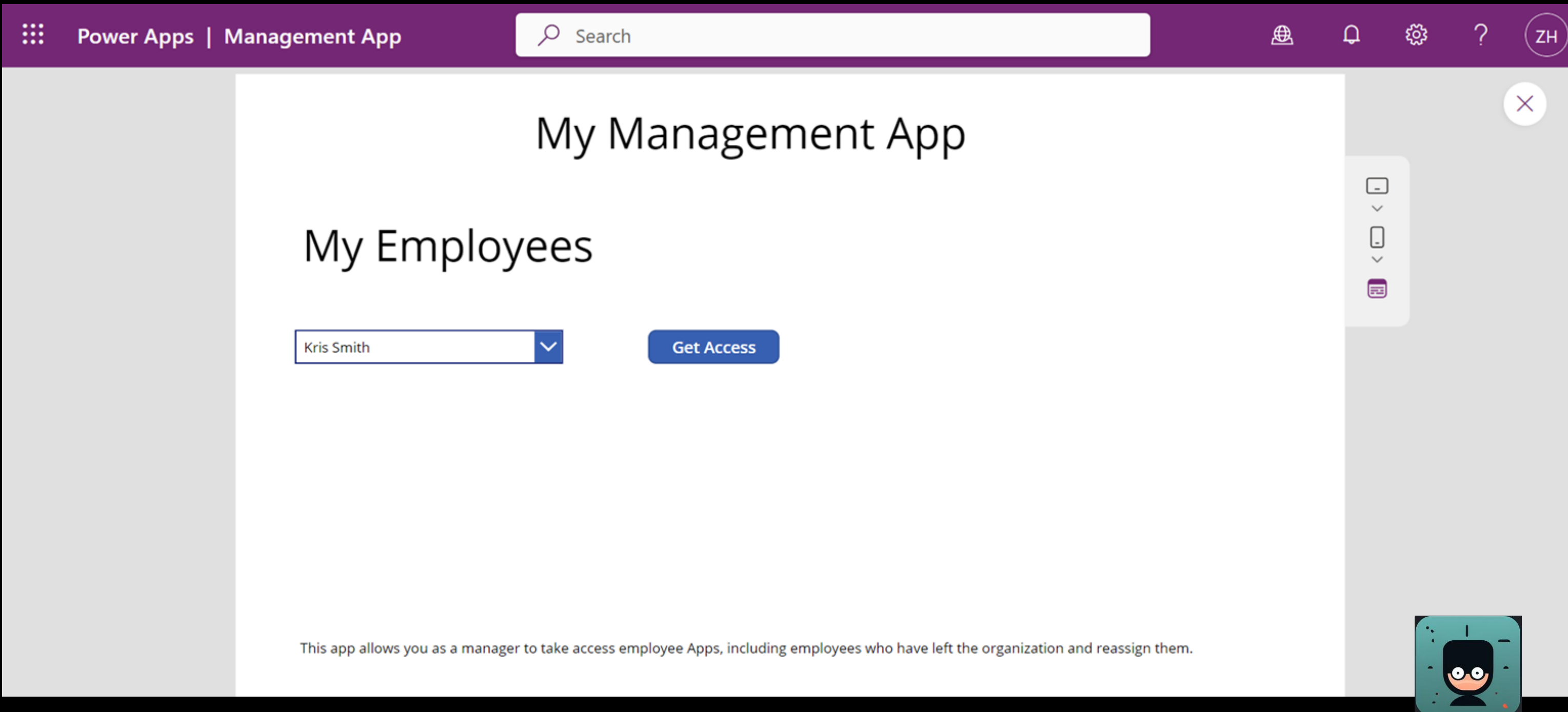


# Story #3 – self-service

# What happens when a maker leaves the org?

# What happens when a maker leaves the org?

- Asset Management Failures



Sure, Let Business Users Build Their Own.  
What Could Go Wrong?

@mbrgO  
BSideLV 2023

Power Automate

Search

Environments  
Zenity Stage (default)

?

ZH

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Get Access to Employee Apps

Undo

Redo

Comments

Save

Flow checker

Test

PowerApps (V2)

Email

Please enter an e-mail address

Add an input

+

Get Apps


Apply to each 2

Apply to each 3

+ New step

Save

Ask a chatbot



Sure, Let Business Users Build Their Own.  
What Could Go Wrong?

@mbrgO  
BSideLV 2023

Power Automate

Search

Environments  
Zenity Stage (default)

Settings

Help

ZH

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Get Access to Employee Apps

Undo

Redo

Comments

Save

Flow checker

Test

PowerApps (V2)

Email

Add an input

Get Apps

Apply to each

Apply to each

Apply to each 3

Select an output from previous steps

value x

Apply to each

Select an output from previous steps

value x email x

Set App Owner

Environment Name

properties/envi... x

PowerApp Name

name x

API Version

2016-11-01

Content Type

application/json

Role For Old App Owner


CanView

New PowerApp Owner

email x

Add an action

Ask a chatbot



Sure, Let Business Users Build Their Own.  
What Could Go Wrong?

@mbrgO  
BSideLV 2023

Power Automate

Search

Environments  
Zenity Stage (default)

Settings

Help

ZH

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Get Access to Employee Apps

Undo

Redo

Comments

Save

Flow checker

Test

PowerApps (V2)

Email

Add an input

Get Apps

Apply to each

Apply to each

Apply to each 3

Select an output from previous steps

value x

Apply to each

Select an output from previous steps

value x email x

Set App Owner

properties.environment x

PowerApp Name

name x

API Version

2016-11-01

Content Type

application/json

Role For Old App Owner


CanView

New PowerApp Owner

email x

Add an action

Ask a chatbot

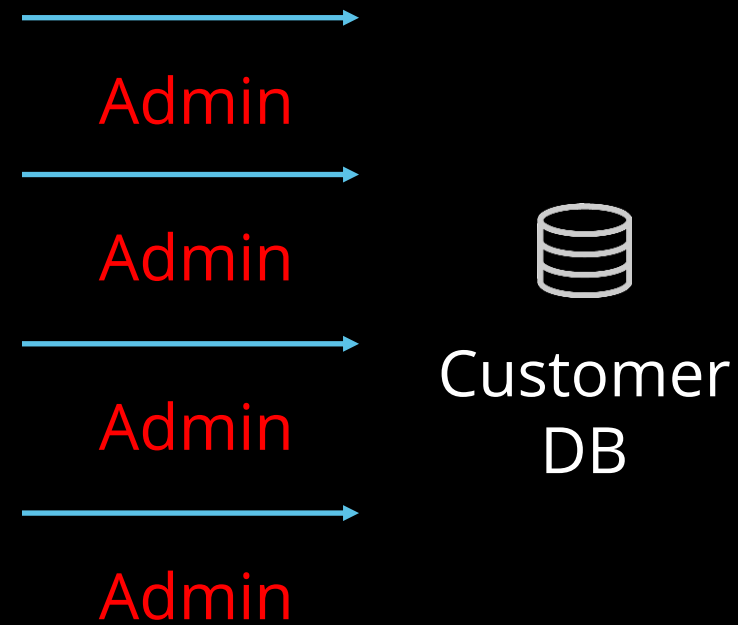


# Self-service – findings



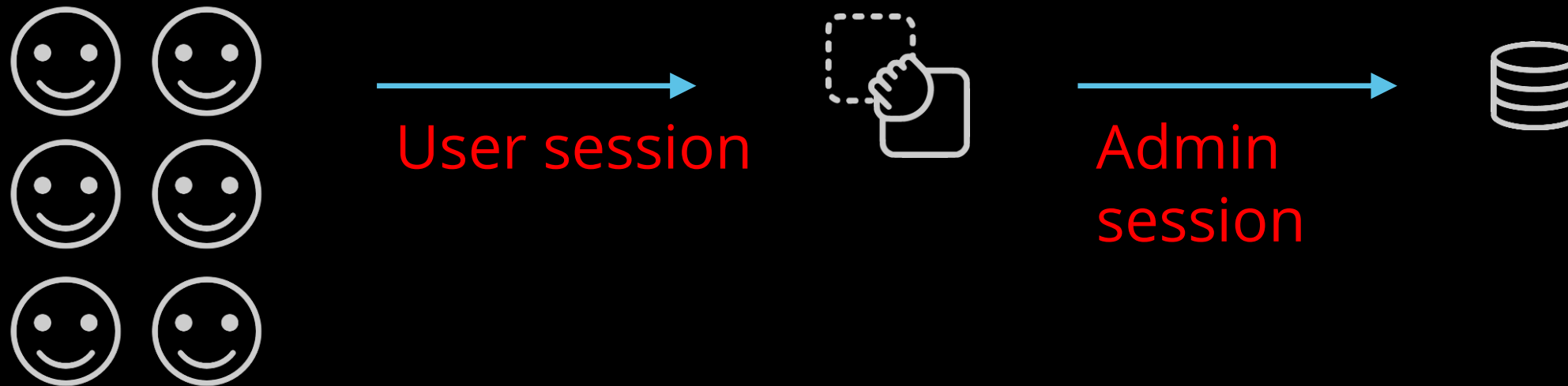
# Self-service – findings

SOC Panics!



# Self-service – findings

- App embedded with admin ID (Account Impersonation)



# My Management App

## My Employees

Kris Smith



**Get Access**

This app allows you as a manager to take access employee Apps, including employees who have left the organization and reassign them.



## What Could Go Wrong?

@mbrg0  
BSideLV 2023

The screenshot shows the Chrome DevTools Network tab. The 'Headers' tab is selected for the first request. The 'X-Ms-Request-Url' header is highlighted with a red box. The URL is: `/apim/logicflows/f818501a-d1ce-42db-873a-5f5261671cc7/triggers/manual/run?api-version=2015-02-01-preview`.

Path	Headers	Payload	Preview	Response	Initiator	Timing
<input type="checkbox"/> /invoke	Sec-Ch-Ua-Mobile: ?0					
<input type="checkbox"/> /Collector/3.0	Sec-Ch-Ua-Platform: "Windows"					
<input type="checkbox"/> /Collector/3.0	Sec-Fetch-Dest: empty					
<input type="checkbox"/> /Collector/3.0	Sec-Fetch-Mode: cors					
<input type="checkbox"/> /powerapps/apps/bc428f80-8f28-4877-a490-f40a0d3cae7...	Sec-Fetch-Site: cross-site					
<input type="checkbox"/> /config/v1/PowerApps/1.0.0.0	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36					
<input type="checkbox"/> /config/v1/PowerApps/1.0.0.0	X-Ms-Client-App-Id: /providers/Microsoft.PowerApps/apps/bc428f80-8f28-4877-a490-f40a0d3cae75					
	X-Ms-Client-Environment-Id: /providers/Microsoft.PowerApps/environments/Default-32f814a9-68c8-4ca1-93aa-5594523476b3					
	X-Ms-Client-Object-Id: 7cb2f429-a54a-46c3-8e4f-df3a3032f249					
	X-Ms-Client-Request-Id: 769a604e-cb2f-4bda-899d-1898d8781bfc					
	X-Ms-Client-Session-Id: 7f7754ee-d98c-43d2-bcff-3c1745ac7cf8					
	X-Ms-Client-Tenant-Id: 32f814a9-68c8-4ca1-93aa-5594523476b3					
	X-Ms-Request-Method: POST					
	X-Ms-Request-Url: /apim/logicflows/f818501a-d1ce-42db-873a-5f5261671cc7/triggers/manual/run?api-version=2015-02-01-preview					
	X-Ms-User-Agent: PowerApps/3.23074.15 (Web Authoring tool; AppName=bc428f80-8f28-4877-a490-f40a0d3cae75)					

7 requests | 2.8 kB transferred | 1.3 kB resources

## What could go wrong:

@mbrg0  
BSideLV 2023

The screenshot shows the Chrome DevTools Network tab. The top toolbar includes search, filters (Preserve log, Disable cache, No throttling), and a filter dropdown set to 'All'. Below the toolbar, a timeline shows two requests: '/invoke' and '/Collector/3.0'. The '/Collector/3.0' request is selected, and its details are shown in the right pane. The 'Request Payload' tab is active, displaying a JSON object: `{email: "zivh@cloudcore.com"}`. A red box highlights this payload. The bottom status bar indicates 2 requests, 1.4 kB transferred, and 0 B resources.



# Self-service – findings

- App embedded with admin ID (Account Impersonation)
- IDOR (Injection handling failures)



# Self-service – findings

- App embedded with admin ID (Account Impersonation)
- IDOR (Injection handling failures)

## Recap:

- We are leaving heavy security decisions in the hands of business users
- When choosing between productivity and security, the choice is obvious

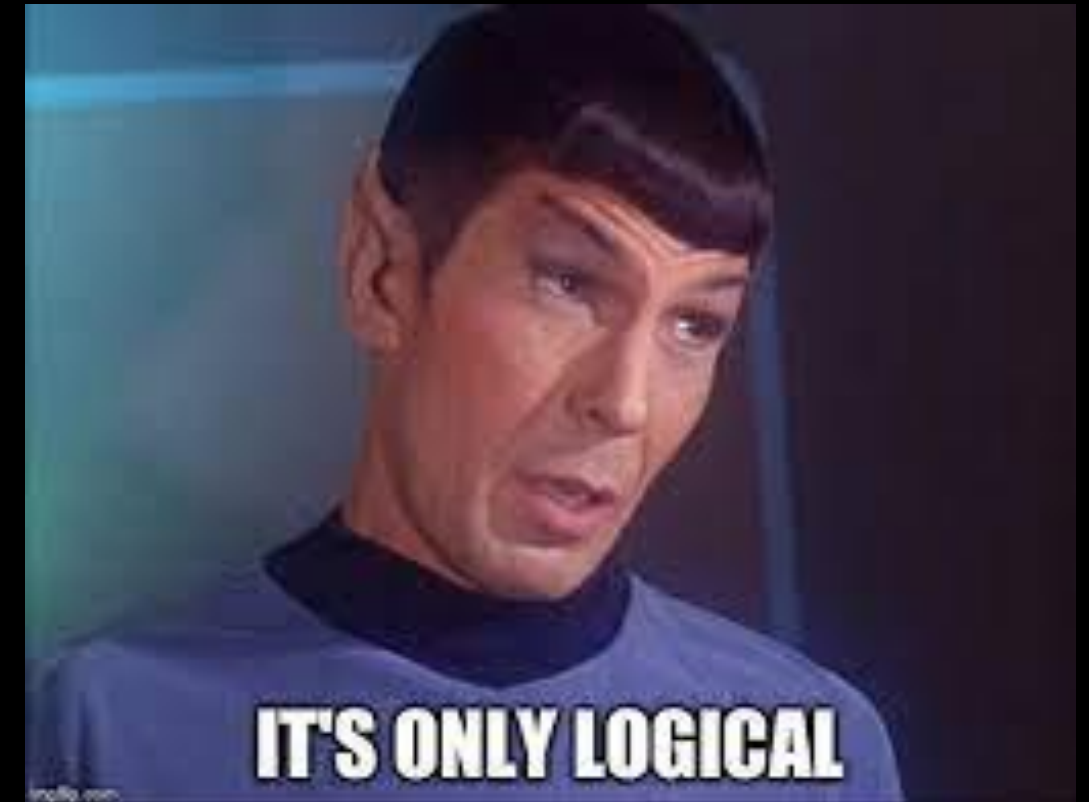


## **We've given business users:**

- **Dev-level power**
- **Missing best practice**
- **No controls**
- **No guardrails**

## We've given business users:

- **Dev-level power**
- **Missing best practice**
- **No controls**
- **No guardrails**



## Could we really expect anything else?

How can we fix it? (Or: LCNC  
AppSec)

# LCNC AppSec is different

AppSec for, well, traditional apps    AppSec for LCNC apps

# LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness

AppSec for LCNC apps

1. Business users w/ no awareness

# LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness
2. Secure SDLC

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC

# LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness
2. Secure SDLC
3. Secure controls

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply

# LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness
2. Secure SDLC
3. Secure controls
4. Hundreds of apps / year

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year



# Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year

# Take the opportunity to champion LCNC security in your org

## AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year

### Example Attack & Misuse Scenarios - Business Users

#### Scenario #1

A developer builds a No Code/Low Code Robotic Process Automation (RPA) application that connects to a database to update records. The connection uses the Admin's authentication (username and password) to log updates. Although 10 different users use this RPA process, all actions are being recorded as being done by the Admin. Logging systems can no longer track productivity, attribute errors to specific users, or identify malicious behavior.

#### Scenario #2

A developer builds an application to help the sales team in the field. The developer uses their credentials (username and password) when writing the application, so all sales made through the application are attributed to the developer, not the sales person facilitating the sale.

OWASP LCNC Top 10 sections for business users by John McTiernan and Yianna Paris  
@punk\_fairybread

# Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year

## LCNC Security Standard:

- Approved use cases
- SDLC
- Environments
- Testing
- Monitoring
- SBOM
- ...

# Take the opportunity to champion LCNC security in your org

## AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year

When a row is added, modified or deleted

```
{
  "headers": {
    "Expect": "100-continue",
    "Host": "prod-52.westeurope.logic.azure.com",
    "x-ms-correlation-request-id": "d7b3daa4-0bba-4724-918b-4523e1bb2e75",
    "x-ms-client-request-id": "d7b3daa4-0bba-4724-918b-4523e1bb2e75",
    "x-ms-user-id": "7cb2f429-a54a-46c3-8e4f-df3a3032f249",
    "Content-Length": "1258",
    "Content-Type": "application/json"
  },
  "body": {
    "cr6e4_email": "daniellds@gmail.com",
    "_owningbusinessunit_value": "edfdf52a-e501-ec11-94ee-0022488300bc",
    "_owningbusinessunit_value@Microsoft.Dynamics.CRM.lookuplogicalname": "bu",
    "_owningbusinessunit_type": "businessunits",
    "statecode": 0,
    "_statecode_label": "Active",
    "cr6e4_sensitiveinputid": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",
    "statuscode": 1,
    "_statuscode_label": "Active",
    "cr6e4_contact": "202-555-0117",
    "_createdby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_createdby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",
    "_createdby_type": "systemusers",
    "cr6e4_dateofbirth": "10.10.1990",
    "ownerid_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "ownerid_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",
    "ownerid_type": "systemusers",
    "modifiedon": "2023-08-07T16:40:48Z",
    "cr6e4_address": "116 E 60TH ST NEW YORK USA",
    "cr6e4_name": "Daniel Wood",
    "_modifiedby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_modifiedby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",
    "_modifiedby_type": "systemusers",
    "cr6e4_ssn": "78051120",
    "createdon": "2023-08-07T16:40:48Z",
    "ItemInternalId": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",
    "SdkMessage": "Create",
    "RunAsSystemUserId": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "RowVersion": "12774383"
  }
}
```

LCNC is an  
opportunity for  
more visibility  
than ever before

# Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year



# Sure, Let Business Users Build Their Own. What Could Go Wrong?

Michael Bargury @ Zenity  
BSidesLV 2023