Chapter 5 – Microsoft as a security provider: From the Word corporation to digital bodyguard

Microsoft has quietly transformed itself from a once-ridiculed office software provider to a heavyweight in IT security. Today, the motto is: connect everything, monitor everything and
as automatically as possible.

In this chapter, we take a look behind the scenes:

How does Microsoft's security strategy work? Who does what, from Entra to Defender to Purview?
And how do these tools interact
to protect companies from real threats?

You will learn:

- What Defender XDR really is
  (spoiler: it's more than just antivirus software)
- How Logic Apps and Azure Functions can be used to automate attack responses
- And why Microsoft Purview is not just a data protection tool, but your best friend when it comes to GDPR, NIS2 & Co.

Microsoft provides the tools,
this chapter shows you what you can do with them.

5.1 Microsoft's security strategy in one sentence: "Connect and monitor everything"

Microsoft has undergone an amazing transformation in recent years:

from an Office manufacturer with a poor reputation for security to a provider of one of the most comprehensive security platforms in the world.

And the goal? It can be summed up in one sentence:

"Connect and monitor everything – as automatically as possible."

This means:

- identities, devices, apps, data, networks and infrastructure – everything is connected
- Every action is recorded, evaluated and analysed
- Deviations from normal behaviour are automatically detected and, in the best case, immediately blocked

Microsoft is not relying on individual tools
but on a platform strategy.

Everything fits together like Lego, only with more security protocols.

Would you like some examples?

- A suspicious login attempt to a Microsoft account -> automatically triggers an alert
- An infected laptop logs into Defender for Endpoint -> blocks itself from the network
- A compromised account ->
  is immediately restricted via Conditional Access
- All data points -> converge in Microsoft Sentinel, the central monitoring centre

And best of all:
Many of these building blocks are already included in Microsoft 365, or can be added as modules.

Sounds like surveillance?

Yes, but in a positive sense.
Because you can only protect what you can see.

And that is precisely Microsoft's security philosophy:

Everything that moves digitally is a potential attack vector,
so we take a close look.

5.2 Azure, Microsoft 365, Entra, Defender, Sentinel, Purview

Microsoft's security landscape often feels like a hidden object game:

Tools, functions, terms everywhere, and somewhere in between: you, with the question "What do I actually need for what?"

So: time for clarity.

Here are the most important components, explained simply:

Microsoft Entra (formerly Azure AD)

The identity centre.

This is where it is decided who you are, what you are allowed to do and where you can access, whether in the cloud or locally.

- Authentication, single sign-on, MFA, conditional access
- Basis for zero trust & identity protection

Microsoft Defender (XDR)

The security army in the background.

Defends devices, identities, data and cloud infrastructure intelligently and in an integrated manner.

Key sub-products:

- Defender for Endpoint
- Defender for Identity
- Defender for Office 365
- Defender for Cloud

Microsoft Sentinel (SIEM/SOAR)

The central observer.

Collects security data, detects attacks, automates responses.

Azure-based, scalable, usage-based

Microsoft Purview

The compliance and data protection compass.

Responsible for data classification, policies, legal requirements, audits and governance.

Includes:

- Data loss prevention (DLP)
- Sensitivity labels
- Insider risk management
- eDiscovery, audit, compliance score
  Absolutely relevant for NIS2, GDPR, KRITIS & CRA