nic X edition

May 31 – June 2, Oslo Spektrum

10th anniversary

Sander Berkouwer
Raymond Comvalius

Increasing the Security of on-premises Active Directory with Azure AD

Sander Berkouwer
Raymond Comvalius

Increasing the Security of on-premises Active Directory with Entra and Defender technologies

Introducing Raymond en Sander

- Raymond Comvalius
  - Independent IT-architect
  - Microsoft Certified Trainer since 1999
  - Windows & Devices for IT MVP since 2011
- Sander Berkouwer
  - CTO at SCCT
  - Enterprise Mobility MVP since 2009
  - Microsoft Certified Trainer since 2014
  - Veeam Vanguard since 2016
  - VMware vExpert since 2018

Agenda

- Only change passwords when you need to
  - Implement multi-factor authentication everywhere
  - Get notified of leaked credentials
  - Ban bad passwords
- Get and stay on top of things
  - Manage the on-premises infrastructure better
    - Azure AD Connect Health for
      - Active Directory Federation Services
      - Active Directory Domain Services
    - Microsoft Defender for Identity
  - Get on top of millions of events
    - Azure Sentinel

The problem with passwords

The problem with your on-premises passwords

- Passwords are problematic
    - Passwords are increasingly being
        - Cracked
        - Stolen
        - Intercepted
        - Eavesdropped
        - Phished
        - Reused
- Passwords are in the way
    - Your colleagues forget their passwords
    - Password resets cost loads of money

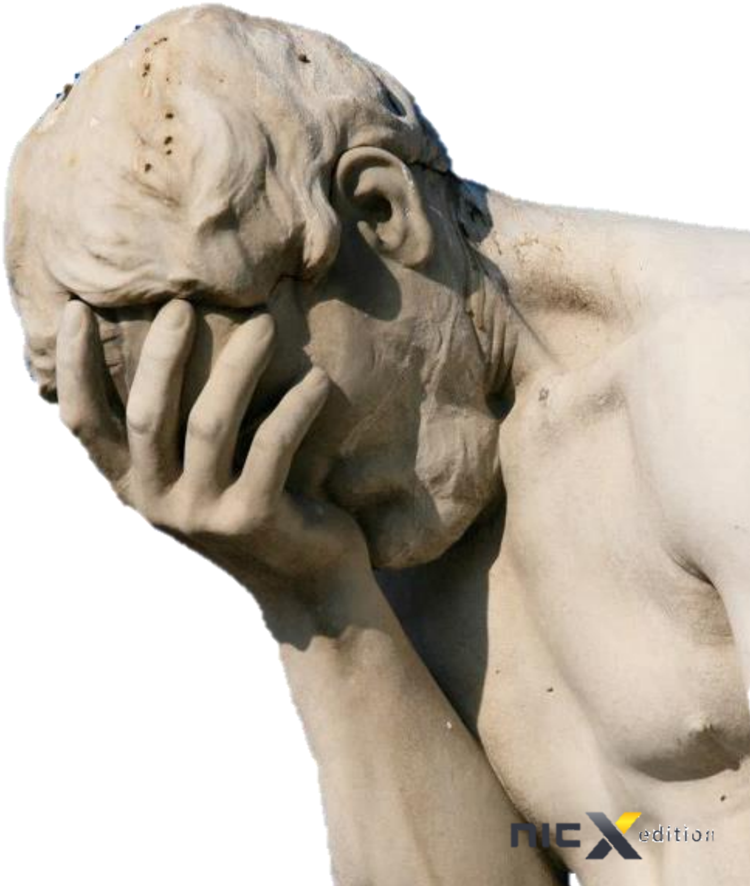
How bad!?

81%

81% of all digital incidents are related to weak or leaked passwords

20%

20% of IT costs for organizations are made to help end users with lost passwords



What can we do?

- Federate applications for single sign-on
  - Every person in your org only needs one account with one password
- Implement self-service password reset
- Implement multi-factor authentication everywhere
- Implement Identity Protection
- Ban bad passwords
- Subscribe to Troy Hunt’s HaveIBeenPwned.com
- Configure passwords for end-users to not expire NIST SP 800-63-3

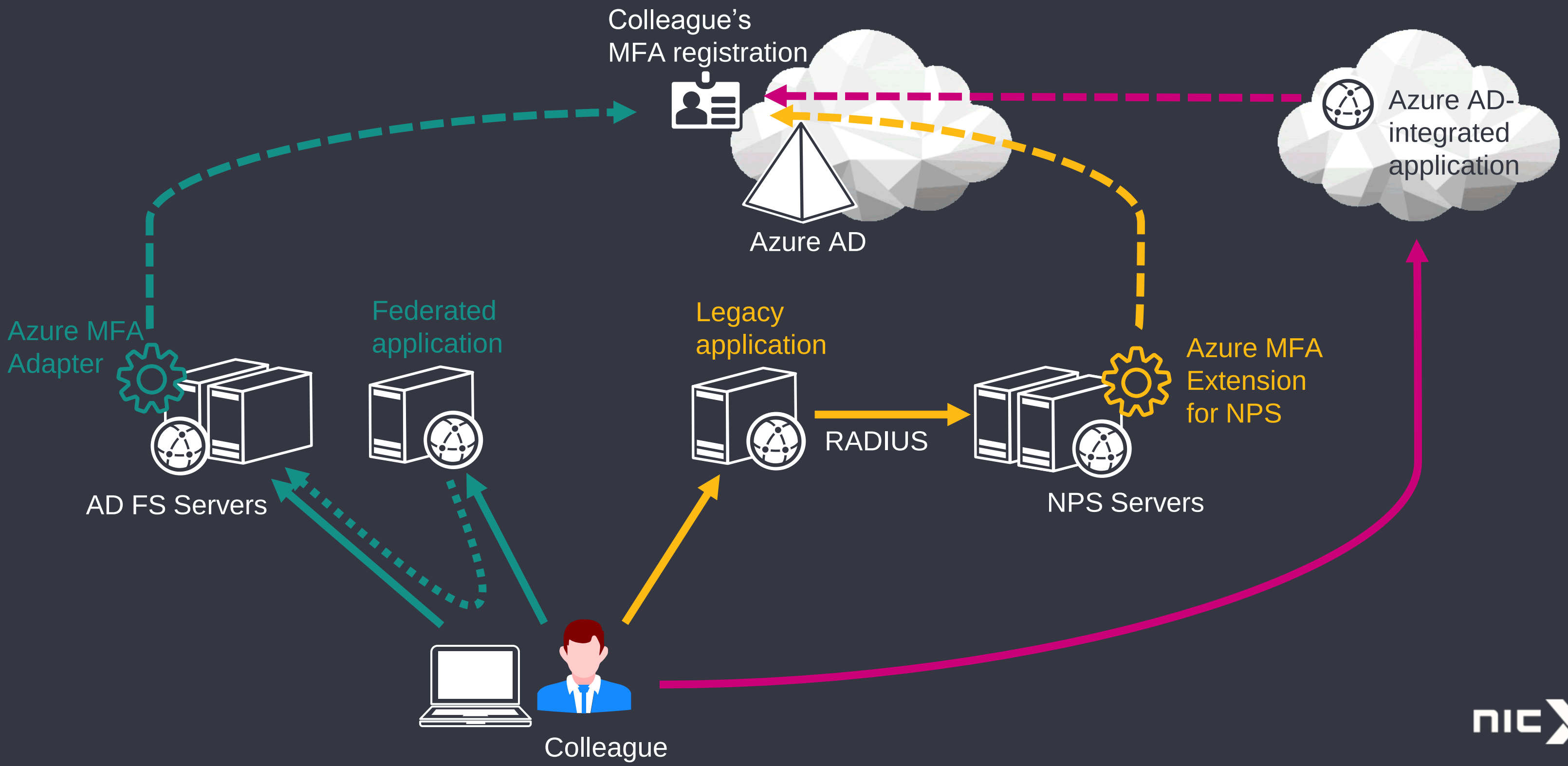
Implement multi-factor authentication everywhere

Multi-factor Authentication from Microsoft

- Azure MFA
  - Azure AD Security Defaults **free**
  - Azure AD Conditional Access
  - NPS Extension for Azure MFA (RADIUS)
  - Azure MFA Adapter for Active Directory Federation Services (AD FS)

- Azure MFA Server Deprecated
  - RADIUS
  - Internet Information Services (IIS)
  - Azure MFA Server Adapter for Active Directory Federation Services (AD FS)

Azure MFA Archictecture



Tips and Tricks

- Enable the combined registration for SSPR and MFA
  It will be automatically enabled for all Azure AD tenants on September 30, 2022
- There is a difference between registering and performing MFA
  - People need to register MFA before it can be required…

Register multi-factor authentication		Require multi-factor authentication	
Security Defaults	14 days grace period	Security Defaults	Based on user risk
Conditional Access	Next sign-in	Conditional Access	Based on conditions
Self-service Password Reset	Next sign-in	Self-service Password Reset	Every use
Identity Protection MFA Registration Policy	14 days grace period	Identity Protection User & Sign-in Risk	Based on user risk

- Don’t use the legacy PhoneFactor portal to require or configure MFA
- Everywhere we mention Azure MFA, you can also use Duo, Trusona, RSA, etc.

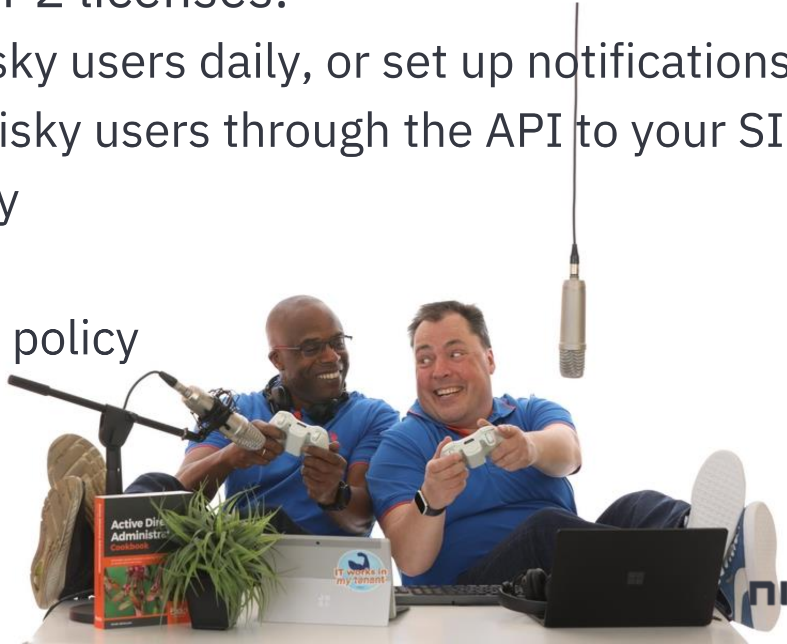
Implement Identity Protection

Azure AD Identity Protection

- Azure AD Identity Protection is enabled for all Microsoft Cloud sign-ins, including Microsoft accounts
- Azure AD leverages AI to flag risky sign-ins
  - Multiple risky sign-ins may result in a risky user
  - These sign-ins are **cloud** sign-ins
- Azure AD leverages leaked credentials to inform admins
  - Leaked passwords are checked when orgs have PHS enabled
  - Admins are notified when sync'ed hashes correspond to calculated hashes
  - Persons with leaked credentials need to change their passwords at next sign-in by default
- Integrated with Conditional Access and Cloud App Security
- Configuration and reporting is part of Azure AD Premium P2

Tips and Tricks

- If you do not have Azure AD Premium P2 licenses
  - Sit back and enjoy the ride
- If you have Azure AD Premium P2 licenses:
  - Check the risky sign-ins and risky users daily, or set up notifications
  - Stream the risky sign-ins and risky users through the API to your SIEM
  - Configure the sign-in risk policy
  - Configure the user risk policy
  - Configure the MFA registration policy



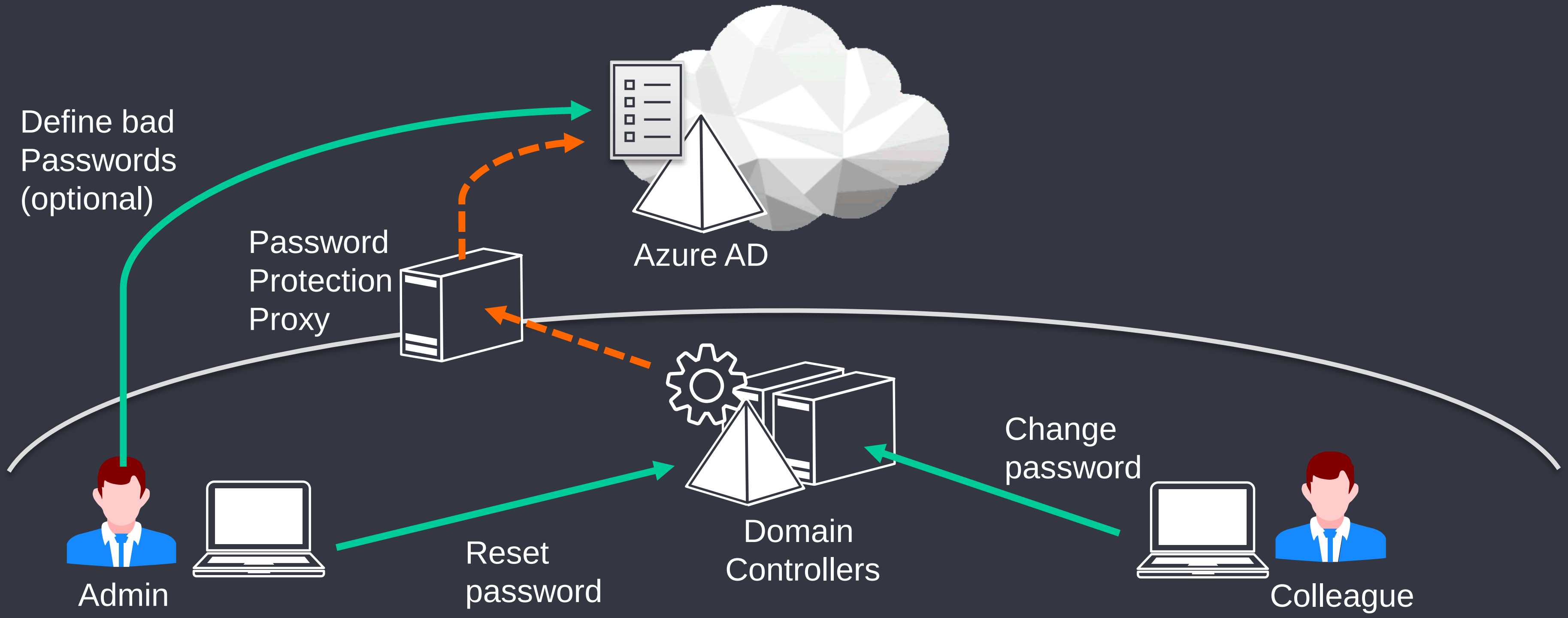
Ban Bad Passwords

Azure AD Password Protection

- Bad passwords are:
  - Weak passwords
  - Passwords that are among the Top 1000 leaked passwords
  - Passwords that are easily guessable
  - Passwords that are reused in leaked services, apps and systems

- Azure AD Password Protection allows you to ban bad passwords
  - Both in Azure AD and on Domain Controllers
  - Admins can set 4+ character words to be banned
    - These easily guessable words cannot be used in passwords

Azure AD Password Protection Architecture



Tips and Tricks

- Install the Password Protection agent on **all** Domain Controllers
  - Ensure .NET Framework 4.7.2 or up is already installed
    - Not part of the Windows Server 2016, needs to be downloaded…
- Use the Audit mode before enabling the Enforce mode
- Ban locations, cities, products and bosses as banned passwords
- Do not ban swear words
  - Password is the only field that is hidden from view, by default 😉

Get and Stay on Top of Things

It’s a hard knock life…

- Admins either:
  - Have no or little visibility in what’s going on
  - Are overloaded with events and notifications
  - Are fighting to keep systems, apps and services work
  - All of the above

- Some notifications are more important than other notifications:
  - Get insights into Hybrid Identity components with Azure AD Connect Health
  - Get insights into common challenges with Defender for Identity
  - Stream all insights to Azure Sentinel

Azure AD Connect Health

Azure AD Connect Health

- Azure AD Connect Health
  - Installed by default on Azure AD Connect
  - Insights into synchronization errors and Azure AD Connect availability
- Azure AD Connect Health for AD FS
  - Synthetic logons to test authentication end-to-end
  - Insights into authentications, traffic and errors
  - Are applications suitable for migration to Azure AD
- Azure AD Connect Health for AD DS
  - Insights into Domain Controller replication and FSMO roles

- Admin requires Azure AD Premium license to start using Azure AD Connect Health
- Admin receives notification when something is wrong
- Admin can use the Azure AD Connect reports to gain insights on usage

Tips and Tricks

- Azure AD Connect Health requires
  - One Azure AD Premium license per Azure AD Connect installation
  - 25 Azure AD Premium licenses in the tenant per
    - AD FS server
    - Web Application Proxy server
    - Active Directory Domain Controller
  - Licenses do not have to be assigned to users, but they can be
- Implement additional Azure AD Connect in Staging Mode when the functionality it offers is critical
  - No automatic failover when actively-sync'ing Azure AD Connect fails
  - Release management
    - Failback to previous version
    - Failback to known good configuration

Microsoft Defender for Identity

Microsoft Defender for Identity

- Previously known as Azure Advanced Threat Protection (Azure ATP)
  - Before that: Advanced Threat Analytics (ATA)
- Manage Identity risks with cloud intelligence:
  - Prevent
    - Identify Active Directory configuration vulnerabilities
    - Get Active Directory remediation guidance
  - Detect
    - Leverage real-time analytics and data intelligence
    - Prioritize and surface real threats, not false positives
  - Investigate
    - Prioritize remediation based on risk levels and prior incidents
  - Hunt
    - Use KQL queries to look for threats across your organization
- Microsoft Defender for Identity requires Microsoft 365/EMS E5 licenses

Microsoft Sentinel

Microsoft Sentinel

- Microsoft Defender for Identity focuses on Active Directory
  But there are so many other areas where detecting risky behavior is helpful
- Azure Sentinel can be your cloud-powered, automatically scaling
  - Security Information and Event Monitoring (SIEM) solution, and
  - Security Automation, Orchestration and Response (SOAR) solution
- Azure Sentinel lives on top of Azure Log Analytics Workspace
- Azure Sentinel integrates with
  - Azure Active Directory
  - Microsoft Defender for Identity
  - Microsoft Defender for Office 365
  - Azure Defender
  - Cloud App Security Broker (MCAS)
  - Your on-premises infrastructure, like firewalls and SNMP-connected devices
  - etc.
- Azure Sentinel is licensed as pay-per-GB-ingested plus pay-per-GB-per-month-retention

Concluding

Begin Today

- Only have colleagues change their passwords when they need to
  - Implement multi-factor authentication everywhere
  - Get notified of leaked credentials
  - Ban bad passwords
- Get and stay on top of things
  - Manage the on-premises infrastructure better
    - Implement Azure AD Connect Health for
      - Active Directory Federation Services
      - Active Directory Domain Services
    - Implement Microsoft Defender for Identity
  - Integrate everything and get on top of millions of events
    - Implement Azure Sentinel

Questions?

Thank you!

ITBros.nl

@ITBrosNL

NextXpert.com	DirTeam.com
@NextXpert	@SanderBerkouwer
www.linkedin.com/in/ RaymondComvalius	www.linkedin.com/in/ SanderBerkouwer

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2022