
VALLEY
IT GROUP
PKN
DER IT-MAßSCHNEIDER
PKN - IT Trendgespräche
Zero Admin - Zero Problem
Günter Nikel - Senior Sales Manager

Ansprechpartner

Christian Kirsch

Windows Security Architect

c.kirsch@pkn.de

+49 30 422692 97

Günter Nikel

Senior Sales Manager

g.nikel@pkn.de

+49 30 422692 43

AGENDA TOP

01	PKN - Das Unternehmen
02	Zahlen, Daten, Fakten
03	Warum sollte man nicht mit Administratorrechten arbeiten?
04	Privilegien contra Berechtigungen
05	Wie überlebt man ohne Administratorrechte?
06	Zeit für Fragen?

Carsten Pehlmann | Senior Sales Manager

PKN
DER IT-MAßSCHNEIDER

ZAHLEN & FAKTEN.

Als Managed Service Provider (MSP) und IT-Systemhaus lösen wir Ihre Probleme rund um die digitale Transformation.

Seit fast 30 Jahren bieten wir moderne und zukunftssichere IT-Lösungen und Services - kombiniert mit umfassendem IT-Know-how für alle Branchen und Unternehmensgrößen.

Seit 05/2022 ein Teil der VALLEY IT GROUP mit flächendeckender Präsenz in der DACH-Region.

BESTER IT-DIENSTLEISTER 2023

COMPUTERWOCHE ChannelPartner

Gründung 1995

DIN ISO 9001:2015

14 Mio. € Umsatz 2023

DIN ISO 27001 ab 09/24

85 Mitarbeiter

24/7 Service & Support

PKN DER IT-MAßSCHNEIDER

Unsere DataCenter

RECHENZENTREN STANDORTE

2 DATACENTER	4x10 GB UPLINK
>6.000 VM's	>16 Pb DATENVOLUMEN
99,99% VERFÜGBARKEIT	24/7 BETRIEB & SUP-PORT
120qm RECHENZENTRUM-FLÄCHE	< 1 STUNDE REAKTIONSZEIT
> 12 JAHRE ERFAHRUNG	

PKN
DER IT-MAßSCHNEIDER

IT-Services

Desktopvirtualisierung
Filesharing
IT-Consulting
Serversysteme
Server-Virtualisierung
Storage-Systeme
Hyperconverged Infrastructure
Mobile Device Management
Managed Services

Digital Office

ELO Knowledge
ELO Vertragsmanagement
Digitales Rechnungsmanagement
ELO Dokumentenmanagement
Digitale Personalakte
Consulting
Bewerbermanagement
Besuchermanagement
E-Mail-Archivierung

Cloud Services

Backup as a Service
DataCenter
IP-Telefonie & UCC
Managed Host Server
Managed Virtual Server
Monitoring as a Service
O365 Backup
Workplace as a Service
Deploy as a Service
Citrix Cloud
Microsoft 365
Multicloud
WiFi as a Service

IT-Verkabelung

Datenvernetzung
Elektro
Planung
Sicherheit

Netzwerktechnik

Netzwerktechnik
Wireless LAN
Wireless Site-Survey

Cyber Security

managed Security Operations Center (SOC)
Cloud Protection MS 365
Advanced Threat Protection
E-Mail-Sicherheit und Verschlüsselung
WithSecure Antivirus Lösungen
Mehrfaktor-Authentifizierung

UNSERE FOKUSPARTNER

Ohne unsere Technologie-Partner wären wir nicht da, wo wir heute sind.

Unser Partnernetzwerk bietet Ihnen umfangreiche Vorteile, vor allem in Bezug auf die tiefgreifende Know-how-Integration in den Bereichen Consulting, Serviceleistungen, Technologie und Inhalte sowie die Bereitstellung von umfassenden Lösungen.

Microsoft Partner – Gold Cloud Productivity, Gold Datacenter, Silver Cloud Platform, Silver Application Development, Silver Small and Midmarket Cloud Solutions

Extreme – DIAMOND PARTNER

FUJITSU – SELECT Expert

REALCLOUD – COMPETENCE PARTNER – GOLD

ENGAGE – FORTINET ADVOCATE PARTNER – Integrator

DELL Technologies – GOLD PARTNER

ELO – certified – BUSINESS PARTNER

WITH secure – Gold Partner

veeam | PROPARTNER Silver Reseller

vmware PARTNER – PROFESSIONAL CLOUD PROVIDER

citrix – Partner – Premier Service Provider

SecurEnvoy – S-Premier Partner.

NUTANIX Partners

UNIFY Partner – Professional OpenScape Enterprise – Authorized Circuit

aruba – a Hewlett Packard Enterprise company

PAESSLER – THE NETWORK MONITORING COMPANY

ARCTIC WOLF

cisco Partner – Select Integrator

JUNIPER NETWORKS – PARTNER ADVANTAGE SELECT

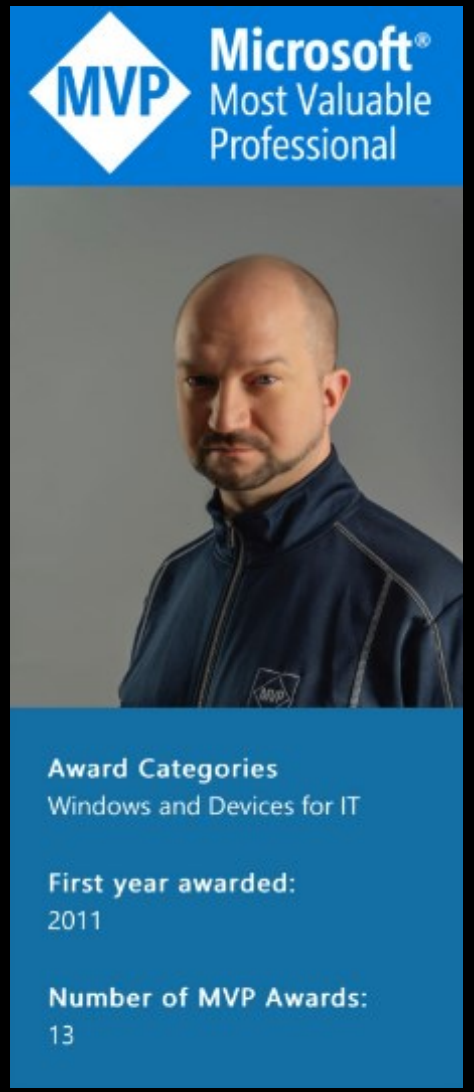
Günter Nikel – Senior Sales Manager

PKN – DER IT-MAßSCHNEIDER

Zero Admins – Zero Problems

Eine Hommage an Sami Laiho der das Thema auf der Microsoft Ignite 2015 präsentiert hat.

Christian Kirsch | Windows Security Architect / Certified Windows Security Master

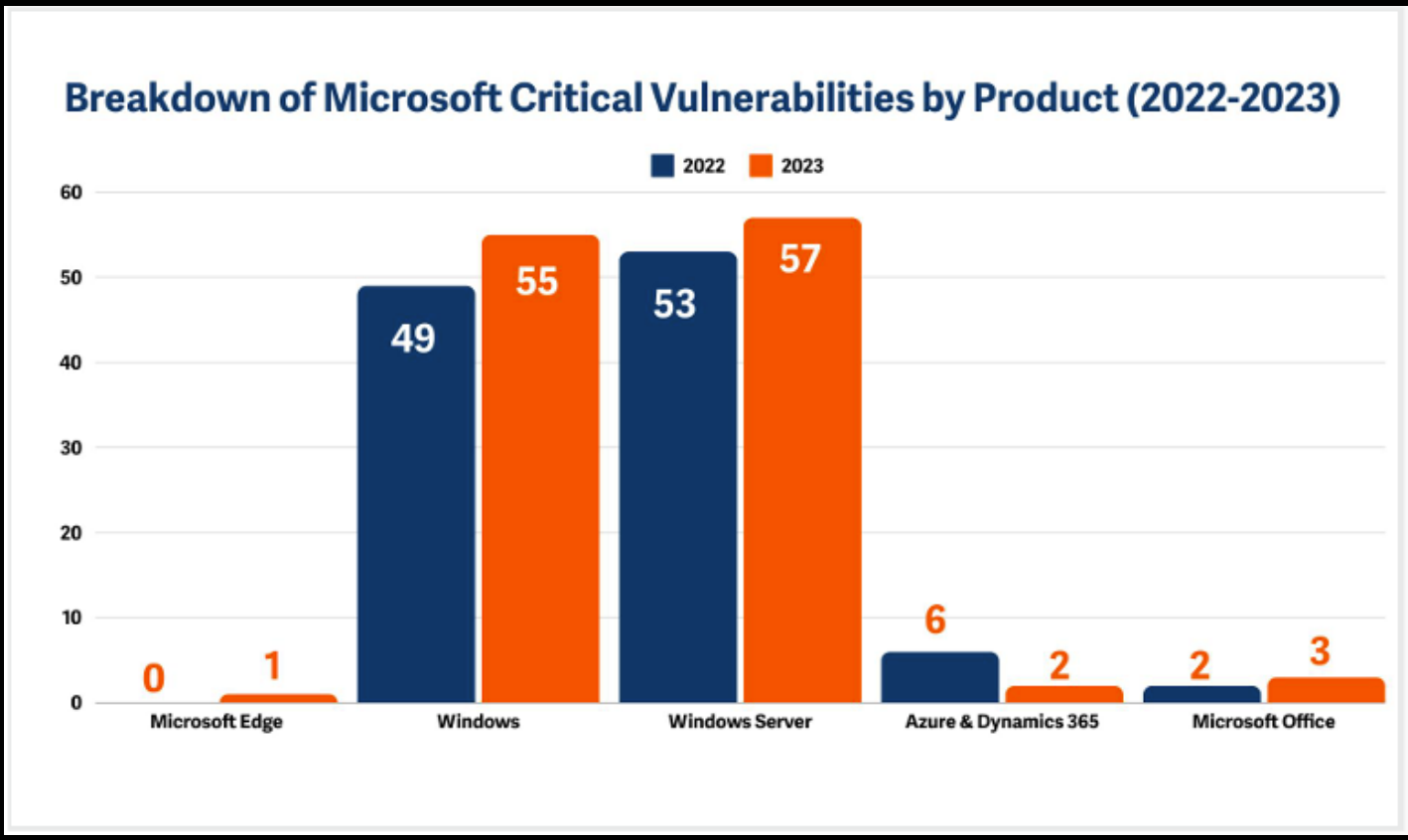


Sami Laiho,

13-facher Microsoft MVP for Windows and Devices
Sami is one of the leading Windows OS professionals in the world. Sami has been working with the Windows OS and training its use since 1995. Sami has been working with companies sized from tens of computers to hundreds of thousands of computers worldwide.

Sami has been auditing and implementing security solutions, specializing in Principle of Least Privilege, Application Control and Privileged Access Workstations, since 2002. Sami has deployed solutions for companies with between 1-550000 endpoints.

Zahlen, Daten, Fakten



The Windows vulnerability category showed a similar pattern, with total vulnerabilities increasing from 513 to 522 (2%), and critical vulnerabilities increasing from 49 to 55.

Quelle: [Beyondtrust Microsoft Vulnerabilities Report]

Experten Meinung

Sami Laiho: *„…With the principle of least privilege, we can still mitigate around half of all critical vulnerabilities, so it is still one of the immutable laws of Windows Security – like the NT 3.1 user guide from 1993 says, there is no security in Windows if you log in as an admin.*

Luckily, Zero Trust (however bad a name it is) has raised the Principle of Least Privilege to most of our lips. Malicious actors need admin rights to run the really dangerous tools, so that is what they are after. As the Microsoft Vulnerabilities Report shows, "Elevation of Privilege accounted for 40% (490) of the total vulnerabilities in 2023." "

Quelle: Beyondtrust Microsoft Vulnerabilities Report

Wie groß ist der Schaden?

Die Schadenssummen, die durch Cybercrime verursacht werden, sind seit Jahren sehr hoch. Laut Branchenverband Bitkom betragen die Gesamtschäden aus Cyberattacken für deutsche Unternehmen im Jahr 2023 mehr als 148 Milliarden Euro. Schäden durch Erpressung mit gestohlenen oder verschlüsselten Daten belaufen sich auf 16,1 Milliarden Euro, was einem Anstieg von 50,5 Prozent entspricht. Weltweit werden bei jedem dieser Fälle im Durchschnitt 577.084 Euro Lösegeld gezahlt. Bundesweit haben im vergangenen Jahr über 800 Unternehmen und Institutionen Angriffe mit Ransomware zur Anzeige gebracht, bei denen Kriminelle schädliche Programme einsetzen, die dem Nutzer den Zugriff auf seine eigenen Daten sperren.

Quelle

Warum sollte man nicht mit Administratorrechten arbeiten ?

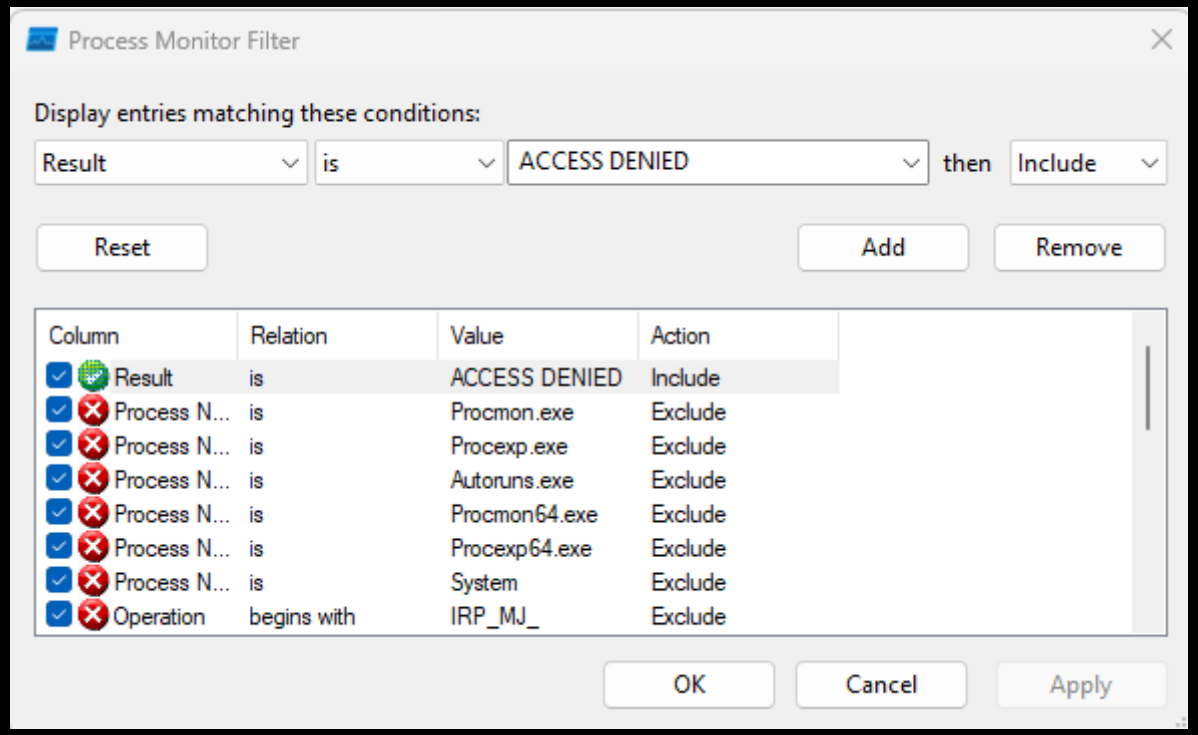
1. Weniger Malware

Die meisten Malware Tools benötigen Administrative Privilegien um ihre Wirkung entfalten zu können.

Die meisten Heimanwender arbeiten als Administratoren auf Ihren Systemen, deshalb sind sie die größte Gruppe, die angegriffen wird.

Und aus diesem Grund machen sich kaum Hacker die Mühe Enterprise Security Konfigurationen zu umgehen, wie zum Beispiel, Credential Guard, AppLocker, BitLocker, etc.

2. Weniger Neuinstallationen



DEMO – Weniger Müll auf dem Datenträger

Principal of Least Privilege

Users: "If I don't have admin rights,
I can't fix my computer"

Reality: "If you don't have admin rights,
you can't break your computer"

3. Security erfordert es

- In der Dokumentation des Betriebssystems, steht das jeder Benutzer der zur lokalen Gruppe der Administratoren gehört, machen kann was er will mit dem Computer / Betriebssystem.
- Gruppenrichtlinien sind nicht dazu gedacht Administratoren zu beschränken.
- AppLocker etc. funktionieren nicht / lassen sich aushebeln für Administratoren.

DEMO – Bypassing Security

BitLocker

Während die meisten BitLocker als Datenverschlüsselungstool betrachten, stellt BitLocker im Kern die Integrität des Betriebssystems sicher. Damit das Betriebssystem nicht manipuliert werden kann.

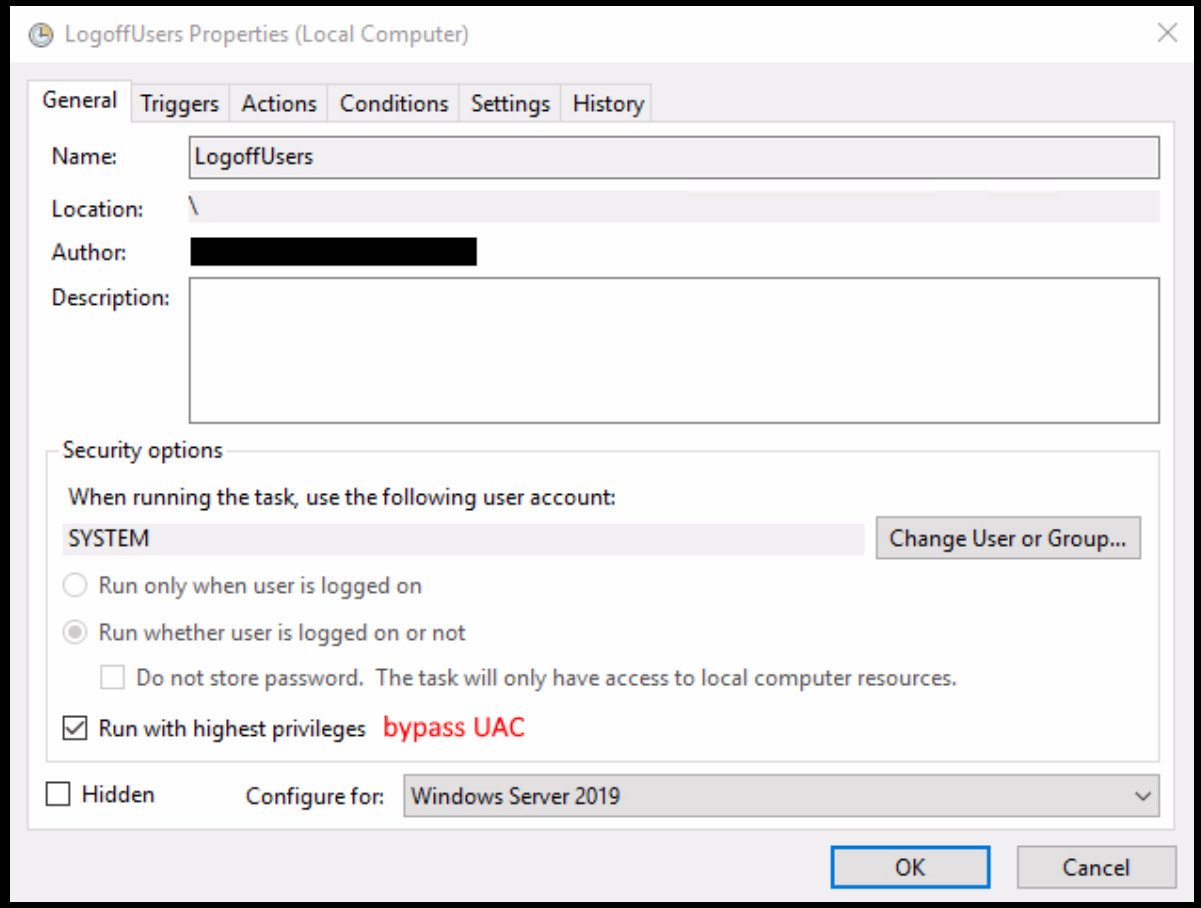
Berechtigungen sind nicht alles !

Wir dürfen nicht vergessen die Berechtigungen, die ein Administrator hat sind nicht wichtig, weil Privilegien immer stärker als Berechtigungen sind.

DEMO – Privileges ROCK !

Wie überlebt man ohne Administratorrechte

Using the SYSTEM-account to elevate things



Elevating processes tokens

Builtin in Windows als native API, kann dazu benutzt werden einen Prozess ohne Veränderung des User Kontextes als Admin zu starten.

=> Es gibt verschiedene Hersteller, die hier für Software anbieten.

„ADMIN RIGHTS ARE NOT HUMAN RIGHTS“

@samilaiho