

dinext.

Group

Portfolio Introduction



Microsoft
Partner



Gold Security
Gold Windows and Devices
Silver Application Integration
Silver Cloud Platform

Gold Security
Threat Protection
Advanced Specialization

Identity and Access Management
Advanced Specialization

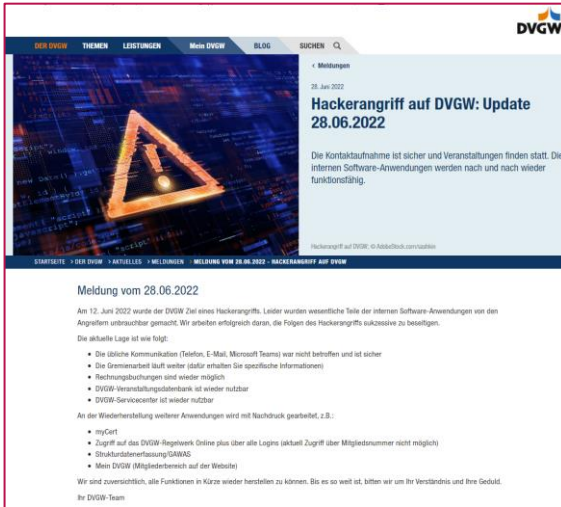
Information Protection and Governance
Advanced Specialization

Member of
Microsoft Intelligent
Security Association



Ransomware as a Service

Pressemitteilungen:



Hackerangriff auf DVGW: Update 28.06.2022

Die Kontaktaufnahme ist sicher und Veranstaltungen finden statt. Die internen Software-Anwendungen werden nach und nach wieder funktionsfähig.

Meldung vom 28.06.2022

Am 12. Juni 2022 wurde der DVGW Ziel eines Hackerangriffs. Leider wurden wesentliche Teile der internen Software-Anwendungen von den Angreifern unbefugterweise gemackt. Wir arbeiten erfolgreich daran, die Folgen des Hackerangriffs sukzessive zu beseitigen.

Die aktuelle Lage ist wie folgt:

- Die übliche Kommunikation (Telefon, E-Mail, Microsoft Teams) war nicht betroffen und ist sicher
- Die Greniarbeit läuft weiter (dafür erhalten Sie spezifische Informationen)
- Rechnungsbuchungen sind wieder möglich
- DVGW Veranstaltungskalenderbank ist wieder nutzbar
- DVGW-Servicecenter ist wieder nutzbar

An der Wiederherstellung weiterer Anwendungen wird mit Nachdruck gearbeitet, z.B.:

- myGert
- Zugriff auf das DVGW Regelwerk Online plus über alle Logins (aktuell Zugriff über Mitgliedsnummer nicht möglich)
- Strukturanforderung/DAMAS
- Mein DVGW (Mitgliedsbereich auf der Website)

Wir sind zusehends, alle Funktionen in Kürze wieder herstellen zu können. Bis es so weit ist, bitten wir um Ihr Verständnis und Ihre Geduld.

Ihr DVGW-Team



Hackerangriff auf Hellmann: Logistiker kappt alle Datenverbindungen

Von Wilfried Hinrichs

10.12.2021, 11:11 Uhr



Osnabrück. Hellmann Worldwide Logistics ist Ziel eines Cyberangriffs geworden. Das bestätigte das Osnabrücker Unternehmen am Freitag. Die Folgen sind noch nicht absehbar.



Hacker legen IT-Systeme des Autozulieferers Eberspächer lahm

Der Auspuffhersteller spricht von einem organisierten Angriff. Auch die Telefonverbindungen sind gekappt. Es ist nicht das erste Mal, dass es ein Familienunternehmen trifft.

Roman Tyboraki Martin-W. Bucherlau

26.10.2021 - 15:00 Uhr • Kommentieren • 6 x geteilt



Cyber-Attacke auf MediaMarkt und Saturn legt Systeme lahm: Mehr als 3000 Server betroffen



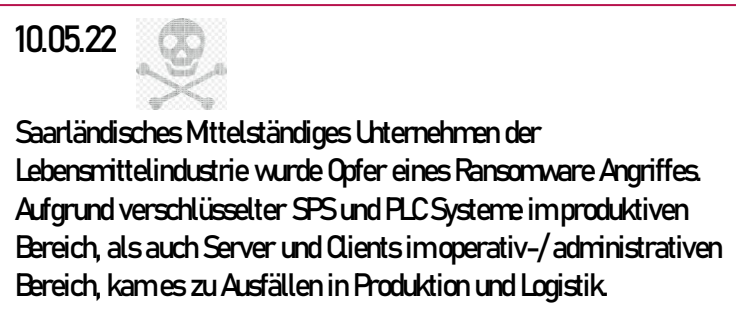
Deutschlandweit sind Märkte von Media Markt und Saturn von einer großen Hacker-Attacke betroffen. Bild: Media Markt


Dienstag, 09.11.2021, 09:21

Nach einem Cyber-Angriff stehen bei MediaMarkt und Saturn die Kassen still. Bargeldloses Bezahlen sei in den Filialen nicht mehr möglich, die Webshops funktionieren weiterhin. An einer Lösung des Problems wird gearbeitet - wie lange das noch dauert, ist unklar.

Fundamental learnings:

- security solutions not holistically deployed.
- disconnected solutions for some geographical locations and entities.
- time to respond and contain too long, because no preparations were made for "major" incident handling.



10.05.22 

Saarländisches Mittelständiges Unternehmen der Lebensmittelindustrie wurde Opfer eines Ransomware Angriffes. Aufgrund verschlüsselter SPS und PLC Systeme im produktiven Bereich, als auch Server und Clients im operativ-/ administrativen Bereich, kam es zu Ausfällen in Produktion und Logistik.

pi-sec solution portfolio



Threat Protection



**Managed Detection
and Response (pi-SOC)**



Incident Response



**Information Protection
& Compliance**

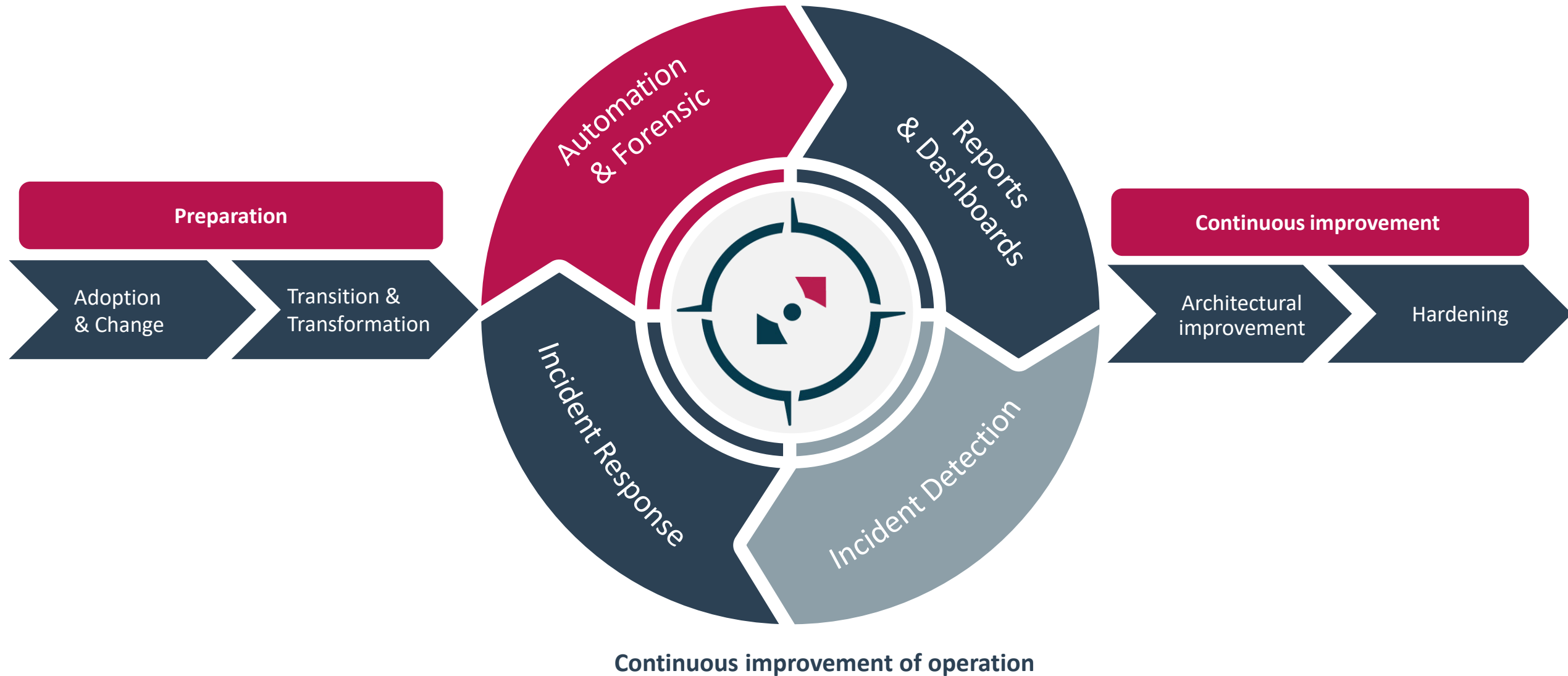


Attack Simulation



**Insights
& Data Science**

Our **transition** approach



Cyber hygiene: the essential part

Key activities at glance:

- Prompt incident investigation and tracking
- Follow up on all alerts
- Adjust detection algorithms
- Vulnerability management workflows
- Be on top of what's happening out there

pi-soc Emotet Update

Alexander Benoit
To: IT Team pliec
Thu 18/11/2021 17:17

General

dinext Emotet - Hunting Guide english.pdf 2 MB
dinext Emotet - Hunting Guide deutsch.pdf 2 MB

Dear customers,
in the last few days, suspicions have been confirmed that a particularly serious type of cyberattack is back. A new variant of Emotet is rolling in via phishing waves.

Earlier this year, Europol announced that it had managed to root out infrastructure of the perpetrators in various countries. However, it was not clear if the perpetrators could be identified.

Emotet:
The name is synonymous with a particularly dangerous type of cyberattack that is "characterized" by mafia-like structures and a high degree of organization. In the past, attackers have successfully managed to attack a wide variety of companies and technically paralyze their IT. The new variant of Emotet is sent primarily via Microsoft Word (.docm) and Excel (.xlsm) files, as well as in password-protected zip attachments. Emotet then uses the infected devices to install spam campaigns and other payloads such as QuakBot (Zbot) and Trickbot. Through these payloads, attackers gain initial access to corporate devices to install ransomware such as Ryuk, Conti, ProLock, Egregor and more.

What can you do?
Currently, very little information is available, but there are indications that certain IPs are used for communication. In addition, there are DLL files associated with the current Emotet loader. Our Pi-Soc analysts found that conspicuous phishing emails of a certain domain arrived in several customer environments. These parameters can be searched for repeatedly in M365 Defender initially and automatically.

Attached to this email are instructions on how to search for these parameters in your M365 Defender and generate automated alerts if results are found in your environment.

If the queries return results, please feel free to contact us immediately for further analysis.

Attached:
• dinext Emotet - Hunting Guide german.pdf
• dinext Emotet - Hunting Guide english.pdf

Best Regards,
dinext pi-soc Team
Alexander Benoit
CEO

Email: Alexander.Benoit@dinext.de
Tel: +49 681983336052
Mobile: +49 151 14802952
Web: www.dinext-group.com

dinext.
Create your digital tomorrow.

dinext pi-soc GmbH | Innovationsring 55 | 66113 Saarbrücken | Geschäftsführung: Alexander Benoit, Philip Waller | Amtsgericht Saarbrücken | HRB 107061



pi-soc Threat Advisory

Microsoft
Partner



Gold Security
Threat Protection
Advanced Specialization
Identity and Access Management
Advanced Specialization
Information Protection and Governance
Advanced Specialization

Microsoft
Partner



Gold Security
Gold Windows and Devices
Silver Application Integration
Silver Cloud Platform

Created by: Giuliano Schneider Alexander Benoit
Date: 11.12.2021

Our transition approach



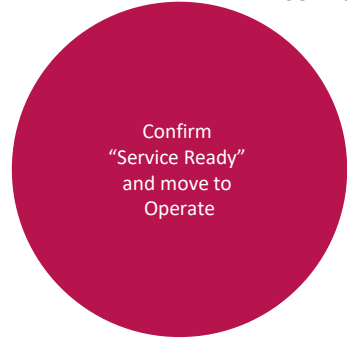
Outcomes

<p>Understanding of customer landscape and priorities</p> <p>High-level customer plan for transition to managed service</p>	<p>Deploy and connect solution, enabling new capabilities</p> <p>Set-up for engaging Security Services for Enterprise</p>	<p>Expert-managed threat detection and remediation</p>	<p>Prepare for incident handling from a processual and technical perspective.</p> <p>Threat modelling and escalation management.</p> <p>Review and lessons learned.</p>
---	---	--	---

Activities

	2-4 weeks	2-4 weeks	3-5 years	ongoing...
<ul style="list-style-type: none"> Align recommendations with customer initiatives and priorities Security Operations Process Review SOC Maturity Assessment 	<ul style="list-style-type: none"> Enable Technology Enable Process Enable People Managed Service setup 	<ul style="list-style-type: none"> Sustained Advisory Services and Service Delivery Management Threat Detection Threat Hunting Threat Remediation Playbook automation Continuous improvement Incident Response + Compromise Recovery 	<ul style="list-style-type: none"> Process review, analysis and documentation Alignment and creation of major incident handling guide Risk Assessment and definition of top threats Disaster recovery, planning and documentation Creation of communication structure for major incident. Security Awareness ISO 27001 prep 	

Decisions



How to get in contact

Alexander Benoit

Patrick Horf



Alexander.Benoit@dinext.de

Patrick.Horf@dinext-group.com