BORIOLI

SWISS CYBER SECURITY

GANZHEITLICHE SCHWEIZER INFORMATIKSICHERHEIT

DEFINITIONEN

Abgrenzung Datenschutz vs. Informations- & Datensicherheit

Informations- und Datensicherheit → Schutz der Organisation (Selbstschutz) → Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit von Daten

Datenschutz → Schutz der Betroffenen (Drittschutz) → Personenbezogene Daten sind betroffen und deren Umgang (Datenverarbeitung)

Was heisst das nun für den Datenschutz?

→ Datenschutz ist Teil von Informations- und Datensicherheit, d.h. ohne Informations- bzw. Datensicherheit kann kein Datenschutz gewährleistet werden.

→ Es muss vor allem auch gemanagt werden → Es braucht also Prozesse, Verfahren & Richtlinien

DEFINITIONEN

Was ist ein Informationssicherheitsmanagementsystem (ISMS)?

«Systematischer Ansatz zur Wahrung und Aufrechterhaltung von **Vertraulichkeit, Integrität und Verfügbarkeit** der Daten mit **angemessenen Mitteln»**.

Norm ISO/IEC 27001:2022 – «Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheits-managementsysteme – Anforderungen»

Wesentliche Kernprozesse eines ISMS:

- Assetmanagement → Inventar erstellen und daraus:
- Risikomanagement für jedes Asset
- Management von Sicherheitsmassnahmen (ISO/IEC 27001: 2022 - Anhang A – Massnahmenkatalog)
- Incident Management → Umgang mit Vorfällen
- PDCA & KVP

ISMS & DATENSCHUTZ

Zusammenhang zu neuem Datenschutzgesetz (revDSG)?

«Verantwortliche und Auftragbearbeiter haben durch Technische und Organisatorische Massnahmen (TOM) eine dem Risiko angemessene Datensicherheit zu gewährleisten».

→ Es ist also zu empfehlen sich mit den wesentlichen Kernprozessen des ISMS zu beschäftigen und den IST-Zustand zu ermitteln:

- Assetinventar erstellen
- Risikomanagement
- Physische & technische Massnahmen checken
- Organisatorische & personelle Massnahmen checken

GREIFEN HACKER SYSTEME AN?

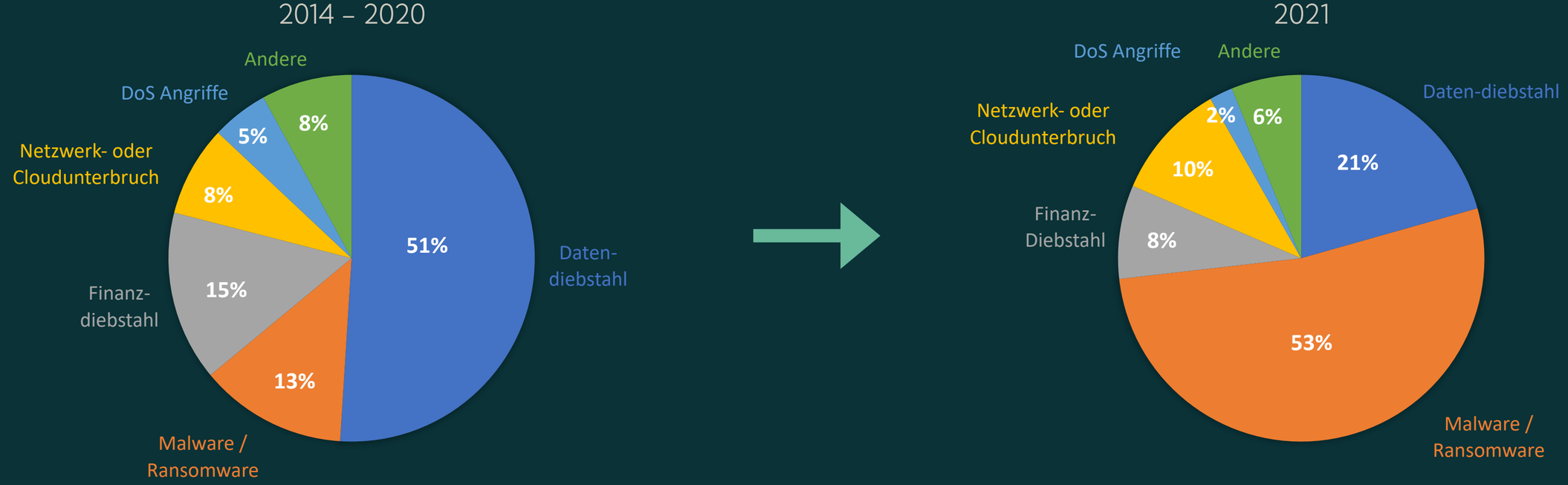
SELTEN - **9 VON 10 CYBERANGRIFFEN STARTEN BEI DEN MITARBEITENDEN.**

ALARMIERENDE SITUATION

> 85%	>90%	> 57%	$ 5.9Mia.	300%
Geräte und IT-Infrastruktur von KMUs werden nicht verwaltet	der gezielten Cyberangriffe beginnen mit einer infizierten E-Mail	der Angriffe werden von herkömmlichen Virenschutz-programmen nicht erkannt	Finanzieller Schaden durch Internetkriminalität im Jahr 2021	Zunahme der Internetkriminalität seit der COVID-19-Pandemie

ANGRIFFSVEKTOREN ÄNDERN SICH

Die Angriffsvektoren haben sich verändert. Ransomware hat im Vergleich zu früheren Jahren stark zugenommen. COVID19 hat das Wachstum nur noch weiter angeheizt. In diesem Bereich hat sich ein eigenständiges, mandantenfähiges Geschäftsmodell entwickelt. Jeder kann heutzutage Ransomware erstellen und verteilen und dabei von den Provisionen für das erpresste Lösegeld profitieren, indem er vordefinierte Ransomware-Tools der führenden Hackergruppierungen verwendet. Diese Zahlen sind im Jahr 2022 erneut gestiegen und wachsen stetig weiter...



WAS BEDEUTET

PHISHING?

GEFAHR PHISHING

EIN ERFOLGREICHER **PHISHINGANGRIFF** ENDET MEISTENS IN EINER **RANSOMWARE-ERPRESSUNG**

RANSOMWARE–ANGRIFF

EIN RANSOMWARE–ANGRIFF HAT ZUM ZIEL, DAS OPFER DURCH ERPRESSUNG ZUR ZAHLUNG EINES GELDBETRAGES ZU BEWEGEN.

EPRESSUNGSSTUFEN IM 2022

STUFE 1 Kompromittierung des Netzwerkes, Diebstahl und **Verschlüsselung der Daten**.

STUFE 2 **Veröffentlichung** und oder **Verkauf der Daten** an die Konkurrenz.

STUFE 3 Zusätzlicher **DDoS-Angriff** auf Ihre Serversysteme.

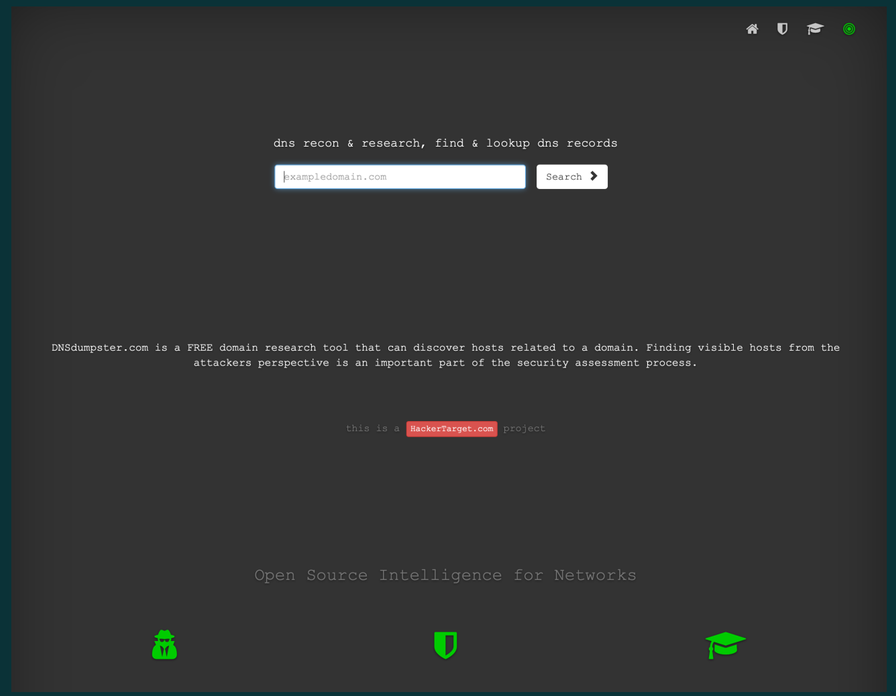
STUFE 4 Kontaktaufnahme und **Erpressung** Ihrer **Kunden** und **Lieferanten**.

STUFE 5 Anruf

RANSOMWARE–ANGRIFF

RISIKEN BEI EINER DATENVERÖFFENTLICHUNG

- FOLGENANGRIFFE
- BENUTZERNAMEN UND KENNWÖRTER
- BANKDATEN
- KREDITKARTEN-INFORMATIONEN
- LIEFERANTENVERTRÄGE
- BETRIEBSGEHEIMNISSE



MYTHOS

ICH BIN FÜR HACKER **UNINTERESSANT**

BERNINA International hacked: ALPHV Ransomware Group Strikes the Sewing Machine Manufacturer

The attack's impact has been felt in the company's offices in Switzerland and Thailand, with tapes and NAS wiped clean. Additionally, the attackers successfully encrypted seven Hyper-V.

by Ashish Khaitan — April 26, 2023 in Data Breach News, Firewall Daily 0

Quelle: https://thecyberexpress.com/bernina-international-hacked/

Ransomware-Bande Play bekennt sich zu Angriff auf NZZ und CH Media

Von Philipp Anz, 17. April 2023 um 16:13

SECURITY CYBERANGRIFF RANSOMWARE PLAY MEDIEN CH MEDIA NZZ

Foto: NZZ

Die Cyberkriminellen drohen mit der Veröffentlichung von "vertraulichen Daten" und Mitarbeiterinformationen. Die beiden Medienhäuser bestätigen uns einen Datenabfluss.

Quelle: https://www.inside-it.ch/ransomware-bande-play-bekennt-sich-zu-angriff-auf-nzz-und-ch-media-20230417

Nach Hackerangriff

Daten des Basler Erziehungsdepartements landen im Darknet

Do 11.05.2023 - 12:41 Uhr
von Maximilian Schenner und tme

Infolge eines Hackerangriffs sind mehrere Datenpakete des Basler Erziehungsdepartements im Darknet gelandet. Insgesamt seien 1,2 Terabyte an Daten hochgeladen worden. Hinter dem Angriff wird die Gruppe Bianlian vermutet.

(Source: lassedesignen / Fotolia.com)

Quelle: https://www.netzwoche.ch/news/2023-05-11/daten-des-basler-erziehungsdepartements-landen-im-darknet

PROFIS HACKEN MENSCHEN

DIE HERAUSFORDERUNG: DER MENSCH IST DAS ZIEL UND AUCH DIE LETZTE VERTEIDIGUNGSLINIE

3.4 Mrd.
Phishing-Mails
werden täglich
versandt

~ 610 Mio.
kommen durch den
SPAM-Filter

~300 Mio.
Phishing-Mails
werden geöffnet!

ANGRIFFSTRENDS 2023

- Künstliche Intelligenz
- Phishing
- Globale Spaltungen und Krisen
- Burnout in Security Teams
- Digitale Supply-Chain-Attacken
- Ransomware as-a-Service
- Multichannel Phishing
- Versagen von Multi-Faktor Authentisierung

CYBERSICHERHEIT FÜR KMU
> KOMPLEX
> TEUER
> UNÜBERSICHTLICH

Ein KMU weiss meistens nicht, wie es vorgehen sollen, um sich zu schützen. Die meisten derer IT-Partner verfügen weder über das entsprechende Spezialwissen und die Erfahrung noch über die erforderlichen Ressourcen. Und die Cyber-Bedrohungen mutieren jeden Tag erneut. Ein Unternehmen zu schützen ist keine einmalige Aktion.

DER LÖSUNGSANSATZ

WIE WIRD DIE CYBERSICHERHEIT FÜR KMU SICHERGESTELLT?

VERLASSEN SIE SICH AUF EINEN INTEGRIERTEN UND VERWALTETEN CYBERSICHERHEITSDIENST, VOLLSTÄNDIG IN DER SICHEREN SCHWEIZER CLOUD BETRIEBEN.

VISION & MISSION

GANZHEITLICHE SCHWEIZER INFORMATIKSICHERHEIT FÜR SIE UND IHR UNTERNEHMEN

Die Sicherheit unserer Kunden hat für uns oberste Priorität. Unser Ziel ist es, mit innovativen Lösungen zur Sicherheit in der digitalen Welt beizutragen - sowohl für Privatpersonen als auch für Unternehmen.

UNTERNEHMEN

Mit diesen Kompetenzen unterstützt die Bortoli AG ihre Kunden:

- Cybersecurity
- Netzwerkinfrastruktur
- Cloud Computing
- Softwareentwicklung
- IT-Support
- Beratung

Die Bortoli AG begleitet Ihre Unternehmung auf dem sicheren Weg zur digitalen Transformation und hilft Ihnen dabei Ihre Daten, Systeme und Prozesse zu schützen.

PRODUCTS & SERVICES CYBER SECURITY SERVICES

PTAAS
Automatisierte Penetrationstests

DIGITALE FORENSIK & INCIDENT RESPONSE
Unterstützung nach einem erfolgtem Angriff. Analyse von Computersysteme und Mobilegeräte.

SOCIAL ENGINEERING ANGRIFFE
In Person Angriffe, Simulierte Phishing-, Vishing- und Manipulationsangriffe

CYBER INTELLIGENCE SERVICES
Investigative Services im digitalen Bereich (Darkweb, OSINT, SOCMINT, e-Discovery)

PHYSISCHE PENETRATIONSTESTS
Simulierte Angriffe auf Ihre Infrastruktur, Mitarbeiter und Prozesse

CONSULTING
Beratung im Bereich Cyber Security. Begleitung bei Rechtsfälle und Erstellung von Expertisen. ISO/IEC 27001 Einführung und Audits.

MASTERMIND®PRO
Security Operation Center und Überwachung (incl. managed Detection & Response)

CYBERDETECTIVE

UMFANG BEREICH IT–SERVICES

NETZWERK LÖSUNGEN
Planung und Installation von LAN-Umgebungen, Wifi, VLAN, Switching und Firewall (inkl. Mikrosegmentierungen)

VOICE
Inbetriebnahme von vPBX und Microsoft Teams Telefonielösungen (wir sind eingetragener VoIP-Provider)

CLIENT- & SERVER LÖSUNGEN
Planen und Installieren von Client- und Serverlösungen, basierend auf Microsoft Technologie und oder Synology NAS.

CYBERPROTECTSHIELD® FÜR KMU
Umfassende, günstige CyberSecurity Gesamtlösung für KMU mit managed Mail Security, EndpointProtection, DLP und vieles mehr.

CLOUD- & MICROSOFT 365
Planen, Migrieren und Einführen von Cloud und Microsoft 365 Gesamtlösungen, hybrid Cloudmodelle und private Clouds.

CONSULTING
Beratung im Bereich Informatikarchitektur, Expertisen und Drittmeinungen, Begleitung als externer Spezialist bei von Dritten durchgeführten IT-Projekte.

IT-BETRIEB & SERVICESDESK
Klassischer Betrieb Ihrer Informatikumgebung mit ServiceDesk, Pikett und diverser SLA‘s.

LÖSUNGSANSATZ

PROFESSIONELLE CYBER SICHERHEITSSERVICES AUS DER SCHWEIZ

> **MANAGED** CYBER SECURITY SERVICES

> **MANAGED** IT SERVICES

BIGPICTURE CYBERPROTECTSHIELD®

CYBERPROTECTSHIELD®

EndPoint Protection	Protection-Management	Backup & Restore	Desaster Recovery	E-Mail Security	Proaktive Überwachung
		Adv. Backup & Restore	Adv. Desaster Recovery	Adv. E-Mail Security	Adv. Proaktive Überwachung & Assessment

AUSBLICK

Was vertiefen wir im nächsten Webinar

- Cybersecurity inkl. Live-Hacking
- Normen ISMS
- Nutzen ISMS-Policy
- Risikomanagementprozess
- PDCA, KVP und Audits

KONTAKT

PHONE +41 31 529 29 00
MAIL INFO@BORTOLI.CH
WWW WWW.BORTOLI.CH

@BORTOLICYBERSECURITY #BORTOLICYBERSECURITY