GBS
A BULPROS COMPANY
Expertise matters

Data Leakage Prevention

Die Top 10 Tipps gegen Datenklau

Schützen Sie Ihr **digitales** Gold »

Datenschutz ist zurzeit in aller Munde. Kein Wunder, denn der eigentliche Firmenwert liegt nicht nur in teurer Infrastruktur, Fertigungsanlagen oder Kapital. Vielmehr sind es die Informationen, die Sie von Ihren Wettbewerbern unterscheiden: den Daten Ihrer Kunden. Das haben längst auch Hacker und Datendiebe erkannt. »

» Bevor Sie jetzt in den Kampf gegen Datendiebstahl ziehen, sollten Sie sich zuerst bewusst machen, welche sensiblen Informationen das Herzstück Ihres Unternehmens sind. Ob Kunden- und Lieferantenlisten, Patente oder Konstruktionszeichnungen - legen Sie fest, welche Informationen Sie als kritisch und absolut schützenswert ansehen.

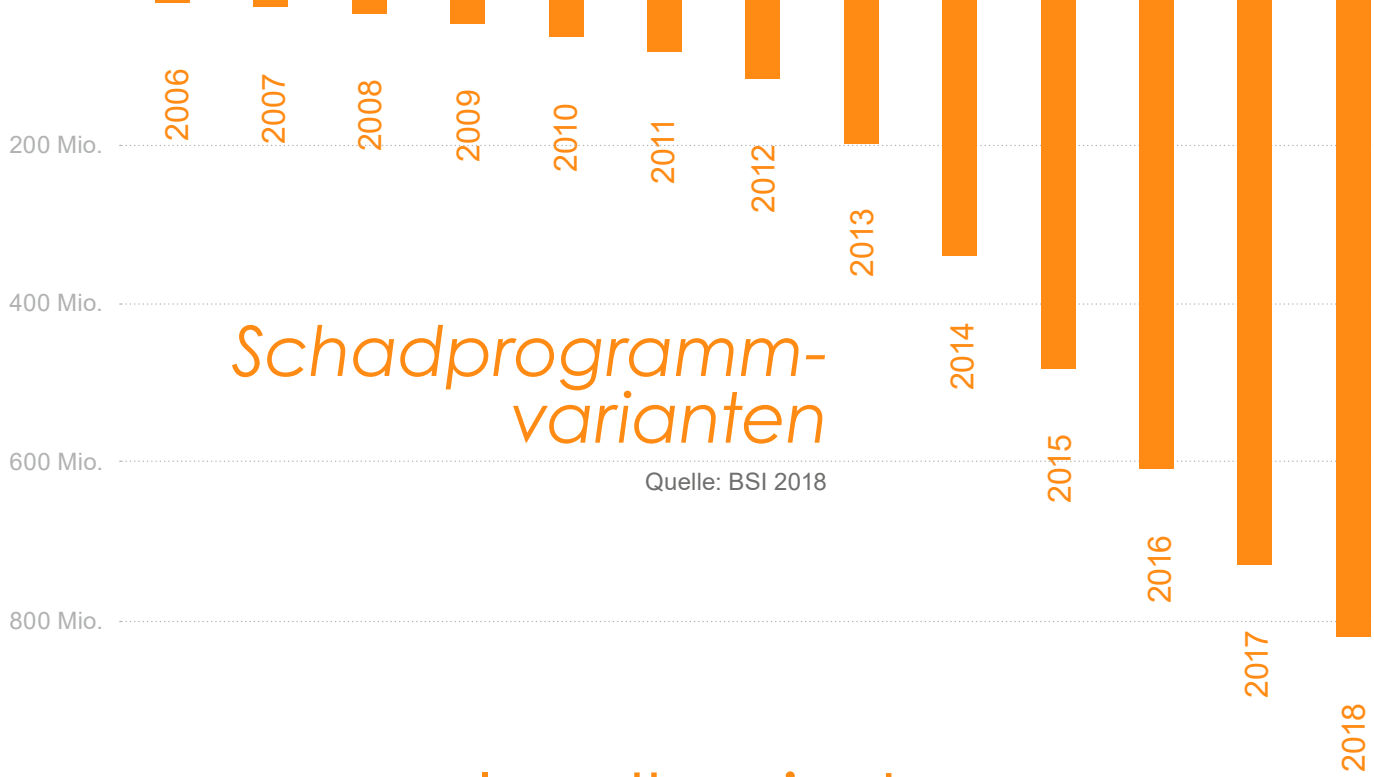
Denn Sicherheit nach dem Gießkannenprinzip ist längst nicht mehr ausreichend. Nur wer erkennt, welche Daten besonders schützenswert sind, kann auch die richtigen Maßnahmen im Bereich Data Leakage Prevention (DLP) ergreifen.

Einer für alle, alle **gegen** Malware »

Das Haupteinfallstor für Hacker sind Schädlinge, die sich meist als harmloser Dateianhang in E-Mails tarnen. Diese sogenannte Malware kann mit einem Klick eine Lawine ins Rollen bringen, an deren Ende Ihre Daten gestohlen werden.

Weltweit gibt es geschätzt über 800 Millionen Schadprogramme und jeden Tag kommen mehrere Hunderttausend neu hinzu. Ein starker Zuwachs ist im Bereich der Makro-Viren zu beobachten, welche sich in Microsoft Office Dateien verstecken.

Der Knackpunkt ist, dass neue Schadprogrammvarianten in sehr großer Zahl und automatisiert entwickelt werden. Die Bereitstellung passender Schutz-Pattern hinkt hier oft hinterher. In diesem Zeitfenster können bisher unbekannte Schadprogramme, sogenannte Zero Day Exploits, nur schwer erkannt werden. »



Schadprogramm-varianten

Quelle: BSI 2018

» Moderne Lösungswege bieten **cloudbasierte** Sicherheitsnetzwerke, mit deren Hilfe aktuelle Bedrohungsinformationen statt innerhalb von Stunden, nun innerhalb von wenigen Minuten zur Verfügung gestellt werden können.

Automatisierung ist **King** »

Schluss mit Insellösungen

Um zu vermeiden, dass Anwendungsfehler Teile Ihrer DLP-Schutzmechanismen außer Kraft setzen und die Mitarbeiter-Produktivität sinkt, ist es unabdingbar den gesamten Prozess zu automatisieren. Setzen Sie statt auf manuell angestoßene Prozesse auf automatisierte Prozesse, denen Ihr persönliches Regelwerk zugrunde liegt. Vertrauen Sie nicht auf Insellösungen, sondern auf ganzheitliche, aufeinander abgestimmte Lösungen, in denen z.B. Spam- und Malware-Prüfung, Phising-Schutz, Erkennung und Kategorisierung sensibler Informationen, 4-Augen-Prüfung und Verschlüsselung automatisiert und zentral ablaufen. Denn gerade im Sicherheitsbereich gilt: Nur ein automatisierter Prozess ist ein guter Prozess!

Nur so können Sie Sicherheit, Produktivität, Akzeptanz und Compliance gewährleisten.

GBS
A BULPROS COMPANY

Phishen Sie nicht im Trüben »

Fast kein Tag vergeht ohne Meldungen über neue Phishing-Angriffe. Ob Paypal, Amazon oder DHL – mit den vollkommen authentisch wirkenden E-Mails wird versucht die Herausgabe von sensiblen Informationen, wie z.B. Passwörtern, zu erreichen. Bleiben Sie also wachsam, um Phishing-Mails nicht auf den Leim zu gehen.

Unbekannter oder seltsamer Absender

Prüfen Sie, ob der Absender vertrauenswürdig ist.
Ein Blick in die Kopfzeile der E-Mail lohnt sich.

Fehlende oder falsche Anrede

Achten Sie auf eine korrekte persönliche Anrede.

Dringender Handlungsbedarf

Seien Sie misstrauisch, wenn Ihnen jemand droht,
z.B. mit dem Sperren Ihres Kontos.

Eingabe von Daten

Geben Sie niemals auf Anforderung PIN oder TAN preis.

Aufforderung zum Öffnen einer Datei oder Links

Vorsicht Trojaner: Öffnen Sie keine Dateianhänge oder Links.
Diese können zu betrügerischen Webseiten führen.


Vier
gewinnt! »

Vier Augen sehen mehr als zwei! Das gilt gerade beim Versand vertraulicher Inhalte. Und nicht immer muss eine böse Absicht dahinterstecken. Oftmals genügt ein Moment der Unachtsamkeit. So ist es wenig verwunderlich, dass bei 55% aller Cyberattacken die eigenen Mitarbeiter involviert sind.

Datenklau verhindern – Aber wie?

Moderne Lösungen für Data Leakage Prevention bieten hier eine intelligente Inhaltskontrolle, mit der Sie automatisch den E-Mail Text oder Dateianhänge analysieren können. So lässt sich beispielsweise der Versand von Kundenlisten oder Kreditkartendaten blockieren. Der Sicherheitsmechanismus wird durch eine 4-Augen-Prüfung abgerundet, bei der eine zweite Person die E-Mail zur Überprüfung erhält und diese freigeben oder endgültig blockieren kann.

Dieses zusätzliche Sicherheitsnetz hilft Ihnen entscheidend dabei, vertrauliche oder geschäftskritische Inhalte vom Versand auszuschließen.

Der **Schlüssel** zur sicheren Kommunikation »

Die besten internen Sicherheitsmechanismen nützen wenig, wenn der Übertragungsweg unsicher ist. Verschlüsselung ist hier das Zauberwort. Denn nur so können Sie verhindern, dass E-Mails durch sogenannte Man-in-the-Middle Angriffe abgefangen und von Hackern mitgelesen werden.

Ob B2B oder B2C: Für jede Zielgruppe gibt es am Markt eine passende Verschlüsselungslösung, die sich je nach Sicherheitsumfang, Komplexität und dem Einsatzszenario unterscheidet.

Wie auch immer Sie sich entscheiden: Jede Verschlüsselungslösung ist besser als keine! »

Mit Verschlüsselung können Sie

Sicherstellen, dass E-Mails vor dem Mitlesen durch Dritte geschützt sind

Überprüfen, ob die E-Mail nachträglich manipuliert wurde

Die Echtheit des Absenders kontrollieren

» Im einfachsten Fall bieten sich webbasierte oder PDF-basierte Verschlüsselungslösungen an. Bei letztgenannten erhält der Empfänger eine verschlüsselte, mit Passwort gesicherte PDF-Datei, welche die originale E-Mail und deren Anhänge enthält. Geöffnet wird diese mit einem separat zugestellten Passwort.


Fliegen Sie
nicht blind »

Wie ernst ist die aktuelle Bedrohungslage? Ist ihr Unternehmen gerade unter Beschuss? Und wer ist der Ansprechpartner für DLP- und Datenschutz-Vorfälle?

Wenn Sie Datenschutz in Ihrem Unternehmen groß schreiben möchten, müssen Sie technisch, organisatorisch und rechtlich gut aufgestellt sein. Eine zentrale Instanz hilft dabei. Das kann auf personell-rechtlicher Ebene der IT-Sicherheitsbeauftragte, Datenschutzbeauftragte oder Compliance-Verantwortliche sein. Auf technischer Ebene helfen Lösungen, welche DLP-Vorfälle erkennen und Ihnen die notwendige Transparenz über Ihre E-Mail-Kommunikation geben.

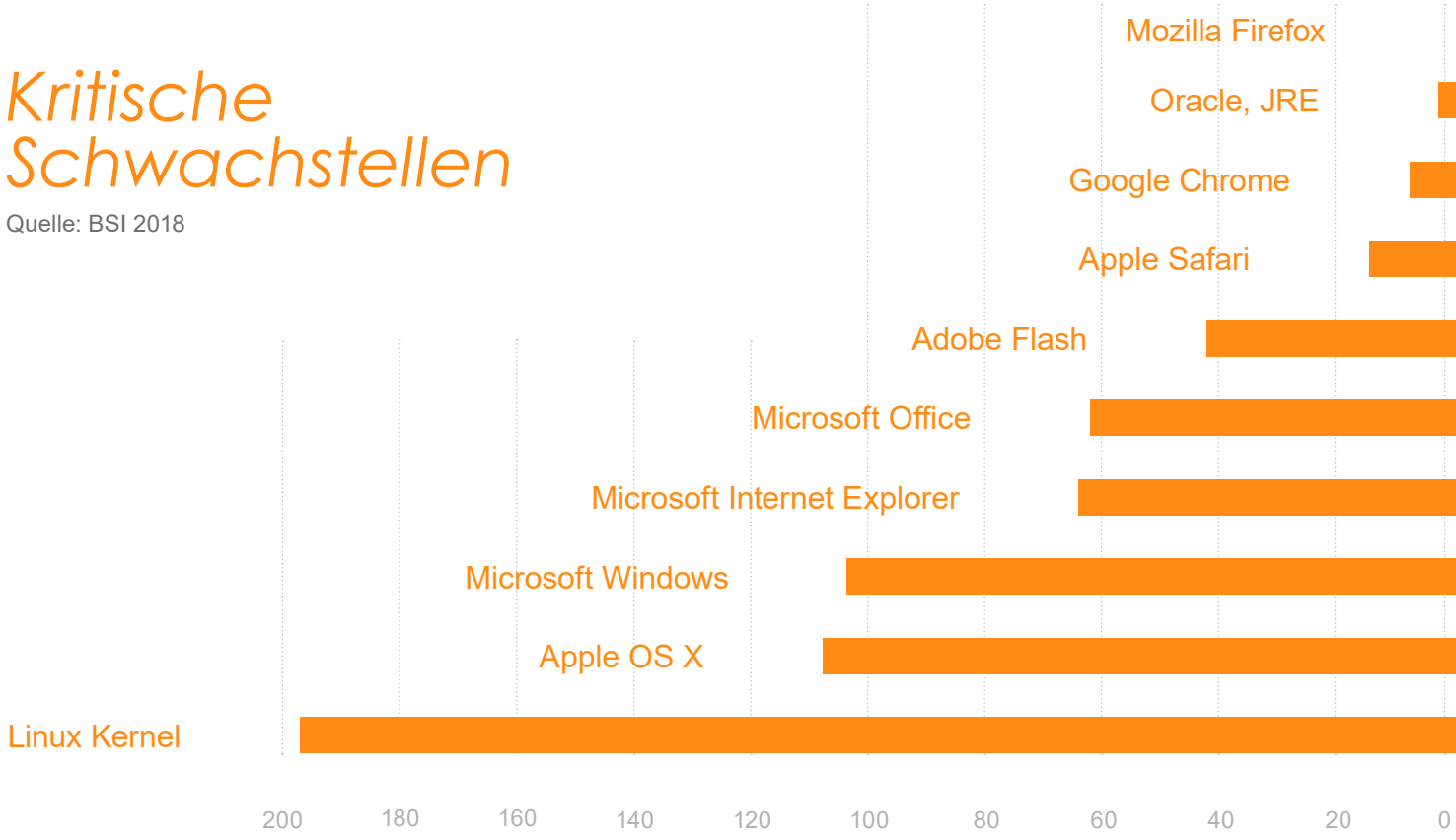
Heute schon **gepatched?** »

Vielen ist es nicht bewusst: Doch die Software, mit der wir täglich arbeiten, beinhaltet Schwachstellen, die von Hackern als Hintertür zu Ihrem Netzwerk genutzt werden können.

Die Anzahl der kritischen Schwachstellen in Standard IT-Produkten ist hoch. Mit Blick auf die 10 am weitesten verbreiteten Software-Produkte war im vergangen Jahr vor allem bei Microsoft Office Produkten sowie bei Linux Kernel ein Anstieg festzustellen. Das regelmäßige und zügige Beheben von Schwachstellen, das sogenannte Patchen, ist daher von großer Bedeutung und keine Option, sondern eine Notwendigkeit.

Kritische Schwachstellen

Quelle: BSI 2018



Legen **Sie** fest,
wie der Hase läuft »

Bringen Sie Licht in den Prozess-Dschungel in Ihrem Unternehmen. Denn nur klar definierte Prozesse mit eindeutigen Verantwortlichkeiten versprechen das notwendige Maß an Sicherheit.

Zusätzlich empfiehlt sich eine Datenschutzerklärung, der alle Mitarbeiter schriftlich zustimmen müssen. Diese dient als Orientierungshilfe und verdeutlicht den Schutzbedarf wichtiger Unternehmensdaten.

Diese Fragen sollten Sie sich stellen

Wer hat Zugriff auf sensible Informationen?

Was geschieht mit Zugriffsrechten, wenn Mitarbeiter das Unternehmen verlassen?

An wen dürfen diese Daten weitergegeben werden?

Welche Informationen sind geschäftskritisch?

Wie dürfen diese Informationen weitergegeben werden?

Wie darf auf diese Daten zugegriffen werden?

GBS
A BULPROS COMPANY

Wissen macht den **Unterschied** »

Ein Viertel aller Cyberattacken geht direkt auf Anwenderfehler zurück. Laut einer aktuellen Cyber-Sicherheits-umfrage des BSI führen jedoch nur 52% der befragten Unternehmen regelmäßige Maßnahmen zur Sensibilisierung ihrer Mitarbeiter durch. »

» Dies erklärt den Erfolg von Täuschungsversuchen, wie den Anrufen von vermeintlichen Microsoft Mitarbeitern: Unter dem Deckmantel einer vorgetäuschten Infektion durch Schadsoftware oder Problemen mit der Windows-Lizenz wurden die Opfer dazu verleitet, eine Fernwartungssoftware zu installieren, über die sich dann Zugang zu Unternehmensdaten verschafft wurde. Angesichts dessen wird deutlich, wie wichtig regelmäßige Schulungen sind.

Um die Sensibilisierung der Mitarbeiter für das Thema Sicherheit zu ermitteln, empfehlen sich über das Jahr verteilte Tests. In diesen wird z.B. gemessen, wieviel Prozent der Testpersonen auf den Link einer präparierten Phishing-Mail klicken. Der Abgleich dieser Messwerte mit zuvor festgesetzten Zielwerten gibt einen guten Anhaltspunkt zur Bestimmung der Wirksamkeit der Schulungsmaßnahmen.

Die Schulung der Mitarbeiter und die Festsetzung von Zielwerten sind Gold wert und sollten neben der Etablierung technischer Schutzmechanismen einen zentralen Stellenwert einnehmen.

Das **Fazit** »

Datenschutz ist heute wichtiger denn je! Doch vor dem Hintergrund der zunehmenden Digitalisierung und immer komplexerer Bedrohungsszenarien stellt das Thema viele Unternehmen vor immense Herausforderungen.

Gefragt ist ein umfassender Prozess, der festlegt wie Informationen durch das Unternehmen zum Empfänger fließen. Basis dafür sind durchdachte und aufeinander abgestimmte Schutzmechanismen und eine ausgeprägte Mitarbeiter-Sensibilisierung. Im Zusammenspiel mit durchdachten Lösungen ergibt sich so aus technischer, organisatorischer und rechtlicher Sicht ein bestmögliches Schutzniveau!

Mit dem Wissen, dass Sie auf allen Ebenen den Schutz Ihrer wertvollen Daten sicherstellen, können Sie entspannt der Zukunft entgegensehen.

Impressum »

Bildnachweis

Titelmotiv:

#100139800	© korionov	Adobe Stock

Inhalt:

#79376533	© Thaut Images	Adobe Stock
#79688936	© alexdemeshko	Adobe Stock
#73576317	© Nomad_Soul	Adobe Stock
#99138434	© Michael Rogner	Adobe Stock
#42944641	© Arman Zhenikeyev	Adobe Stock
#85247200	© shocky	Adobe Stock
#49594504	© mdworschak	Adobe Stock
#64926141	© Yuriy Shevtsov	Adobe Stock

Herausgeber

GBS Europa GmbH
Ottostraße 4
76227 Karlsruhe

Tel.: +49 721 4901-0
expert@gbs.com
www.gbs.com

www.gbs.com