CYBERSECURITY
EXPERTS ON YOUR SIDE

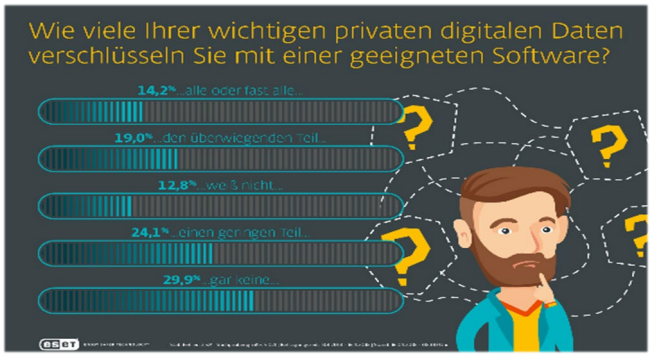
Datenverschlüsselung: ja oder nein? Ein umfassender Faktencheck

Deutsche sind laut einer Umfrage des europäischen Security-Herstellers ESET Verschlüsselungsmuffel. Dies hat sich seit der Einführung der Datenschutzgrund-verordnung in 2018 nur leicht verbessert. Neue Impulse erhält die Diskussion durch die Corona-Krise und der einhergehenden Verlagerung der Geschäftstätigkeit vieler Angestellten ins Home-Office. Denn auch dort müssen betriebliche Informationen sicher vor fremden Blicken geschützt sein.

Was könnte ein Unternehmen mit 20 Millionen Euro anstellen? Aufgeschobene Investitionen nachholen, das Bürogebäude modernisieren oder das Gehalt der eigenen Angestellten aufstocken. Oder – wie ein großes deutsches Internet-Unternehmen – als Bußgeld an nationale Aufsichtsbehörden wegen Verstößen gegen die Datenschutzgrundverordnung (DSGVO) entrichten. Damit steht der Beklagte nicht allein da: Seit Inkrafttreten der Datenschutzgrund-verordnung im Mai 2018 wurden bisher 160.000 Verstöße gemeldet und geahndet. Die Rechtsanwaltskanzlei DLA Pieper beziffert den Gesamtwert der Strafen auf 114 Millionen Euro.

Die Gründe der vielen Verfehlungen sind vielfältig. Letztlich wurde eine elementare Frage nur rudimentär beantwortet: Wie kann man die digitalen Schätze zum Wohle aller schützen und vor allem datenschutzrechtlich korrekt durchführen? Vom Prinzip her gibt es nur drei Möglichkeiten. Entweder man schließt den Zugang zu den Daten bombensicher ab oder man verschlüsselt sie. Idealerweise macht man beides. Leider geschehen alle drei Varianten zu selten. Ansonsten würden nicht laufend lange Listen – unverschlüsselt - mit Benutzernamen plus Passwort oder Kreditkartennummern inklusiv Kennziffern gestohlen werden - und dann im Darknet kursieren, verkauft und von Kriminellen eingesetzt werden.
Der Dumme ist letztlich der Anwender, der seine Daten einem Unternehmen anvertraut hat. Und dies im guten Glauben, dass sie dort sicher seien wie Gold in Fort Knox. Eine Verschlüsslung setzen fast alle Anwender voraus und werden oftmals bitter enttäuscht. Dabei spielt es offensichtlich keine Rolle, ob es sich beim Datenspeicher um einen Groß-konzern oder einen Gewerbetreibenden handelt.

Vielleicht findet bei den großen Sündern bereits ein Umdenken statt. Denn ethisches Handeln, vor allem beim Thema „Datenverarbeitung“ und Nutzung, wird für Menschen/Kunden/Anwender immer wichtiger. Wie die Frankfurter Allgemeine Zeitung treffend feststellte, ist Datenschutz ein Menschenrecht. Immer mehr Personen sehen genau das als wichtige Prämisse. Parallel zum Thema „Nachhaltigkeit“ in der Konsumgesellschaft wächst auch das menschliche Bedürfnis nach Datensicherheit stetig. Und die Verschlüsselung gehört als elementarer Bestandteil dazu. Dies gilt vor allem für betriebliche Informationen – unabhängig davon, ob sie im Büro oder im Home-Office bearbeitet werden.



Juristische Fragen

Muss überhaupt verschlüsselt werden?
Grundsätzlich besteht kein Muß zur Verschlüsselung. Die gültige Datenschutzgrundverordnung nimmt aber Organisationen in die Pflicht, personenbezogene Daten angemessen zu schützen. Im Erwägungsgrund 83 der DSGVO – „Sicherheit der Verarbeitung" – sind die Anforderungen klar definiert:

„Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau – auch hinsichtlich der Vertraulichkeit – gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.

Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte."

Eine Maßnahme, die ausdrücklich in Artikel 32 zur Sicherheit der Verarbeitung personenbezogener Daten genannt wird, ist die Verschlüsselung. Sie wird als geeignete technische Maßnahme empfohlen und anerkannt. Wenn Angreifer alle Hürden wie Firewall, Antiviren-Software oder weitere Sicherungslösungen überspringen, ist eine gute Verschlüsselungslösung das letzte Bollwerk. Sie sorgt dafür, dass nach einem Datendiebstahl Cybergangster zumindest keinen Profit aus den Informationen ziehen können – und die Vertraulichkeit der Daten bewahrt bleibt.

Wer glaubt, auch ohne Verschlüsselung am Markt agieren zu können, für den hält die DSGVO eine Fülle von Anforderungen und verschärfte Strafandrohungen bereit. Und die haben es in sich: Wenn es zu einer Datenschutzpanne kommt, sind saftige Bußgelder fällig, die sogar die Existenz eines Unternehmens gefährden können.

Auch das Bundesdatenschutzgrundgesetz (BDSG) trifft klare Aussagen, wie mit vertraulichen Daten zu verfahren ist. Paragraph 64 BDSG (neu) – „Anforderungen an die Sicherheit der Datenverarbeitung" – geht ins Detail und fordert:

- Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle)
- Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)
- Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle)

Die Verschlüsselung erscheint vor diesem Hintergrund als effektivste und effizienteste Maßnahme. Sicherlich bieten sich für die Umsetzung der Punkte auch andere Maßnahmen an. Diese dürften aber mehr zeitlichen Aufwand und finanzielle Mittel erfordern.

Welche Auswirkungen hat es, wenn man nicht verschlüsselt?
Wer den Zugang zu gespeicherten Informationen bombensicher gestaltet, kann auch ohne Verschlüsselung agieren. Doch wehe, wenn es schiefläuft: Neben dem Verlust der Daten (und damit vielleicht auch der Geschäftsgrundlage) drohen immense Strafen durch die Datenschutzgrund-

verordnung. Vom Image- und Reputationsschaden bei Kunden und Geschäftspartnern ganz zu schweigen.

Weitere Probleme kommen noch aus ganz anderer Richtung. Ein Beispiel: Ohne Verschlüsselung keine Cyberversicherung! Vermeintlich Pfiffige denken möglicherweise, sich teure Investitionen in Sicherheitstechnologien sparen zu können und stattdessen eine Cyberversicherung abzuschließen. Was hilft besser gegen Schäden durch Hacker und Kriminelle als eine Versicherungs-Police. Doch hier wird die Rechnung ohne den Wirt gemacht. Denn die Anbieter setzen Sicherheitsstandards voraus, die der Leistungsnehmer erbringen muss. Und genau in diesen Punkt spielt die Verschlüsselung – oft in Verbindung mit der Zugangskontrolle durch Zwei-Faktor-Authentifizierung – eine entscheidende Rolle. Ohne diese Schutzmaßnahme bleibt der Kunde wohl auf seinem Schaden sitzen, sofern ein Vertrag überhaupt zustande kommt.

Wer hingegen seinem umfassenden Sicherheitssystem die Krone aufsetzen möchte, der liegt mit einer Cyber-Police richtig. Diese sichert die Restrisiken ab und macht zumindest die finanzielle Seite IT-bedingter Ausfälle erträglich.

Fragen aus der Praxis

Warum wird oftmals nicht verschlüsselt?
Unter vielen Antworten hören Experten eine sehr oft: „Ich habe Angst, dass ich den digitalen Schlüssel verliere und nicht mehr an meine Daten komme.“ Tatsächlich war das in der Vergangenheit ein großes Problem insbesondere für Gewebetreibende und kleinere Betriebe. Sie widmeten ihre Zeit lieber Kunden und Klienten als der Technik. Doch dieses ist bereits benutzerfreundlich und dennoch sicher gelöst worden. Die unnötige Furcht, die besonders bei eher wenig technisch versierten Anwendern vorherrscht, hält sich hartnäckig.

Im Unternehmensumfeld spielt dies nur eine untergeordnete Rolle. Hier stellt sich eher die Verfahrensfrage, wie man Daten so verschlüsselt, dass nur eine berechtigte Gruppe der Anwender darauf zugreifen kann. Mit zunehmender Netzwerkgröße an Personal und Daten potenziert sich nämlich das Problem des Schlüsselmanagements. So darf beispielsweise die Personalabteilung per se nicht auf Vertriebsdaten zugreifen. Aber wenn das Gehalt und der Bonus eines Vertriebsmitarbeiters berechnet werden muss, ist der Zugriff sehr wohl wichtig. Nicht nur für den/die eigentliche Sachbearbeiter(in), sondern auch für deren Vertretungen bei Abwesenheit.
Schon müssen Ausnahmen erstellt werden, die aber nur in bestimmten Fällen zum Tragen kommen. Man kann sich vorstellen, wie kompliziert sich dies in Netzwerken mit vielen Teilnehmern aus unterschiedlichen Abteilungen ausgestaltet. Dabei sind die Vorgaben durch die Datenschutzgrundverordnung noch nicht einmal berücksichtigt.

Logischerweise gehen viele Unternehmen dazu über, nur einen Teil der gespeicherten Informationen zu verschlüsseln. So lässt sich der Arbeitsaufwand begrenzen und dennoch ein gesundes Maß an Sicherheit herstellen. Hier liegt die Kunst eher darin, die richtigen Daten zu codieren und den berechtigten Personen zuzuordnen. Selbstverständlich gibt es bereits Lösungen, die alles automatisch verschlüsseln und dies mit der Rechtevergabe durch Microsoft Active Directory koppeln. Mit letzterer umgeht man die Zuordnung der Rechte zu jedem Benutzer. Doch das hat seinen Preis: Wenn jede benutzte Datei

ständig ent- und verschlüsselt wird, erzeugt das eine enorme Netzwerklast. Die dafür benötigten Ressourcen von Hardware bis zum Stromverbrauch treiben die Kosten in ungeahnte Höhen.

Was ist wichtiger, Datenträgerverschlüsselung oder Datenverschlüsselung?

Keine ist wichtiger. Hauptsache, es wird überhaupt verschlüsselt. Eine Datenträgerverschlüsselung sollte auf jeden Fall auf mobilen Geräten Pflicht sein. 3.300 Laptops gehen allein an europäischen Flughäfen verloren – wöchentlich. Damit zählt der mobile Rechner zu den Top 10 der am meisten verloren gegangenen Dinge. Und das nur knapp hinter Sonnenbrille und Schlüsselbund.

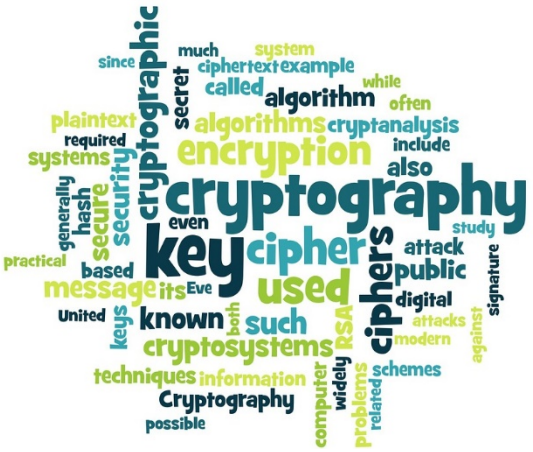
Der physische Verlust des Geräts ist für seinen Besitzer in erster Linie ärgerlich. Auf den zweiten Blick entsteht für Selbstständige wie auch für Unternehmen ein sehr ernstes Problem. Außer den Kosten für eine Neuanschaffung droht auch das Abhandenkommen von wertvollem Know-how, wichtigen Betriebsinformationen, Zugängen zu Netzwerken und Konten oder sogar Kundendaten. Die Folgen können verheerend sein.

Nicht nur personenbezogene Daten (als Massenware) sind von hohem Wert. Besonders der Schutz „digitaler“ Güter wie Know-how und Expertise, Geschäftsgeheimnisse wie Patente und Pläne und aber auch simple Planungsdaten unterliegen in den seltensten Fällen einem ausreichendem Schutzkonzept.

Der große Vorteil der Datenträgerverschlüsselung liegt in der einfachen Bedienbarkeit. Produkte wie ESET Full Disk Encryption lassen sich in wenigen Minuten installieren und ins Netzwerk integrieren. Für den Anwender verändert sich quasi nichts: Er muss beim Booten des Geräts lediglich sein Benutzername und Kennwort eingeben – so, wie er es sowieso bislang machen sollte.

Welche Verschlüsselung ist denn überhaupt sicher?

Die richtige Verschlüsselung ist aktuell (und auch noch für eine recht lange Zeit) eine korrekt implementierte AES 256-Routine. Dieser Standard ist weltweit anerkannt und kann auch offiziell zertifiziert werden. Streng genommen erfreut sich AES 256 so großer Beliebtheit, dass sogar AES Instruktions-Sets in allen aktuellen CPUs enthalten sind oder sogar in der Hardware von Festplatten zum Einsatz kommt. Das führt neben der hohen Sicherheit dazu, dass der Speicher bei den Rechenoperationen kaum beeinträchtigt wird. Hinzu kommt, dass AES noch nie in der Praxis gehackt wurde. Es gibt bekannte Attacken, die aber nur unter „Laborbedingungen“ mit Modellrechnungen vorgenommen wurden. Experten sind sich sicher, dass auch Quantencomputer, sollten sie denn mittelfristig auf den Markt kommen, vorerst nichts ändern werden.



Wie viele Hersteller gibt es in der Europäischen Union?

Der Markt an Verschlüsselungssoftware ist in den vergangenen Jahren stark gewachsen. Auch Hersteller aus der EU agieren erfolgreich am Markt. Doch nicht jeder nutzt eine selbst programmierte Lösung. Viele Anbieter verwenden Microsoft Bitlocker als Basis und veredeln diese nach ihren Vorstellungen.

Der Aspekt „Software aus Europa“ ist zwischenzeitlich nicht nur aufgrund der Einhaltung des Anspruchs von DSGVO-Konformität oder einem gewissen Qualitätsgedanken geprägt, sondern vermehrt auch aus Gründen der nationalen/gefühlten Sicherheit.

Unternehmen aus den USA z.B. unterliegen noch immer diversen Vorgaben (siehe Cloud Act, Privacy Act etc.), um Zugriff auf diverse Daten einzufordern. Das Vertrauen in nicht-europäische Unternehmen ist daher nicht uneingeschränkt gegeben und wird durch aktuelle politische Erfahrungen/Vorkommnisse weiter eingeschränkt. Nicht nur regierungsnahe Organisationen gehen verstärkt dazu über, Produkte von nicht europäischen Herstellern abzulösen.

Sicherheitstechnische Fragen

Kann Verschlüsselung vor Malware oder Ransomware schützen?
Nein. Vor Malware kann nur eine entsprechende Software schützen. Mit der Verschlüsselung der eigenen Daten kann der Anwender – egal ob privat oder dienstlich – lediglich verhindern, dass Fremde diese Informationen lesen und verarbeiten können. Aus dem erbeuteten „Datenwirrwarr“ können Kriminelle keinen Profit schlagen. Je mehr Personen oder Unternehmen verschlüsseln, desto uninteressanter wird das zwielichtige Geschäftsmodell Datenklau und -verkauf. Und führen möglicherweise zu weniger Cyberangriffen mit dieser Zielvorgabe.

Bei Ransomware verhält sich die Sachlage etwas anders. Die Angreifer zielen nur darauf ab, Informationen selbst zu verschlüsseln und über eine Lösegeldforderung Geld zu erbeuten. Dabei spielt es keine Rolle, ob die Daten zuvor bereits codiert waren – am Inhalt sind die Kriminellen nicht interessiert. Auch hier kann nur eine wirksame Sicherheitslösung helfen, Verschlüsselung jedenfalls nicht. Aber schaden kann sie auch nicht.

Reicht die Verschlüsselung heutzutage aus?
IT-Verantwortliche sollten über den Tellerrand hinausschauen. Verschlüsselung sorgt nur für zusätzlichen Schutz, wenn sie auch genutzt wird. Und das wird sie nur, wenn die Bedienung die Mitarbeiter weder von der täglichen Arbeit abhält noch IT-Sicherheit komplizierter macht.
Die Krypto-Strategie eines Unternehmens sollte sich folglich nahtlos in das IT-Security-Konzept einfügen und die Compliance nicht unnötig aufblähen. Greifen Endpoint-Security, Zwei-Faktor-Authentifizierung und Verschlüsselung ineinander, entsteht eine ganzheitliche Sicherheitsstrategie, die Malware-Angriffe und Ausspäh-Aktionen verhindert und vertrauliche Firmendaten schützt.

Reicht die Windows-Anmeldung aus?
Nein, definitiv nicht. Die Windows-Anmeldung bietet weit weniger Sicherheit als vielfach gedacht. So mancher Windows-Anwender vertraut lieber einer trügerischen Sicherheit: Windows sei doch bei der Anmeldung durch die Eingabe von Benutzername und Passwort geschützt. Dummerweise dient sie weniger dem Schutz der Daten als vielmehr der Verwaltung der verschiedenen Benutzerprofile. Für halbwegs fortgeschrittene Anwender ist es ein Leichtes, über entsprechende Tools Zugriff zu erlangen oder gleich die gesamte Festplatte zu kopieren. Wenn man diesen Weg wählen möchte, ist eine Zwei-Faktor-Authentifizierung unabdingbar.

Sind Cyberversicherungen sinnvoll?
Aus unserer Sicht ist eine Cyberversicherung für Unternehmen sinnvoll, die mit sensiblen Daten arbeiten und ihr Geschäftsbetrieb von deren Verfügbarkeit abhängt. Sie tritt dann für Schäden ein, die im Zusammenhang mit Internetkriminalität entstehen. Nach einem Malware-Angriff zahlt der Versicherer beispielsweise für die Datenrettung oder kommt für die Kosten auf, die mit der vollständigen EDV-Wiederherstellung anfallen. Daneben garantieren die Anbieter weitere Hilfe, die meist als "Assistanceleistungen" ausgeschrieben sind.

Unternehmen sind gut beraten, sich die verschiedenen Vertragsbedingungen genau anzuschauen. Einfach eine möglichst günstige Versicherung abzuschließen, bedeutet nicht, dass alle Schäden einfach so ausgeglichen werden. Hier gilt es, im Vorfeld die passenden Bausteine auszusuchen, die wirklich abgesichert werden müssen. Je mehr die Versicherung leisten soll, desto teurer wird sie.
Einem Irrtum unterliegt auch derjenige, der glaubt, dass die eigenen Anstrengungen und Investitionen in IT-Sicherheit verringert werden können. Genau das Gegenteil ist der Fall: Versicherungsnehmer sind gezwungen, den aktuellen Stand der Technik – auch in der IT-Sicherheit - einzusetzen. Dies kann unter Umständen bedeuten, dass investiert werden muss, bevor eine Police zum Abschluss kommt.

CYBERSECURITY
EXPERTS ON YOUR SIDE

ESET ist ein europäisches Unternehmen mit Hauptsitz in Bratislava (Slowakei). Seit 1987 entwickelt ESET preisgekrönte Sicherheits-Software, die bereits über 110 Millionen Benutzern hilft, sichere Technologien zu genießen. Das breite Portfolio an Sicherheitsprodukten deckt alle gängigen Plattformen ab und bietet Unternehmen und Verbrauchern weltweit die perfekte Balance zwischen Leistung und proaktivem Schutz. Das Unternehmen verfügt über ein globales Vertriebsnetz in über 200 Ländern und Niederlassungen u.a. in Jena, San Diego, Singapur und Buenos Aires. Für weitere Informationen besuchen Sie www.eset.de oder folgen uns auf LinkedIn, Facebook und Twitter.

Folgen Sie ESET:
https://www.ESET.de
https://www.welivesecurity.de
https://twitter.com/ESET_de
https://www.facebook.com/ESET.DACH