IM RAHMEN DER NEUEN DSGVO-VORSCHRIFTEN:

Die Geschichte zweier Ransomware-Angriffe

Seit dem Inkrafttreten der DSGVO am 25. Mai 2018 sind Datenschutzverletzungen bei personenbezogenen Daten finanziell und verfahrenstechnisch so schmerzhaft für Unternehmen und Dienstleistungsanbieter, dass diese jedwede Maßnahmen zur Vermeidung ergreifen werden. Das ist zumindest das Ziel.

Zahlen Sie lieber kein Lehrgeld – sehen Sie stattdessen selbst, wie viel ein wenig Extraschutz leisten kann, um Ihr Unternehmen vor hohen Bußgeldern für Compliance-Verstöße gegen die DSGVO zu schützen.

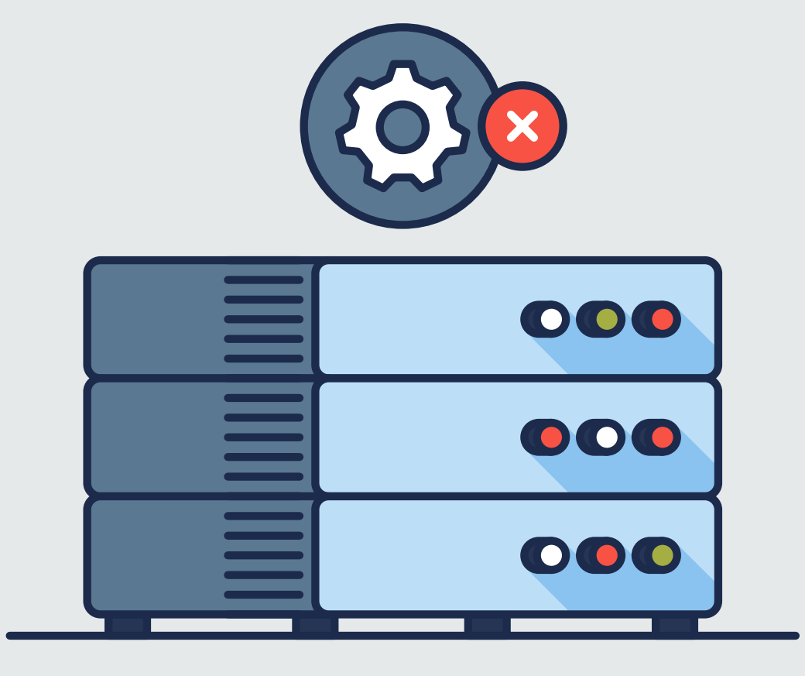
UNTERNEHMEN X

GROẞES RISIKO, GROẞE REUE

Bei ihren Bemühungen, die Auflagen der DSGVO zu erfüllen, übersehen viele Unternehmen eine der gängigsten und wachstumsstärksten Sicherheitsverletzungen von personenbezogenen Daten: Ransomware-Angriffe.

Hier sehen Sie den derzeitigen Verlauf bei einem Angriff:

SCHUTZ VOR RANSOMWARE WIRD IGNORIERT

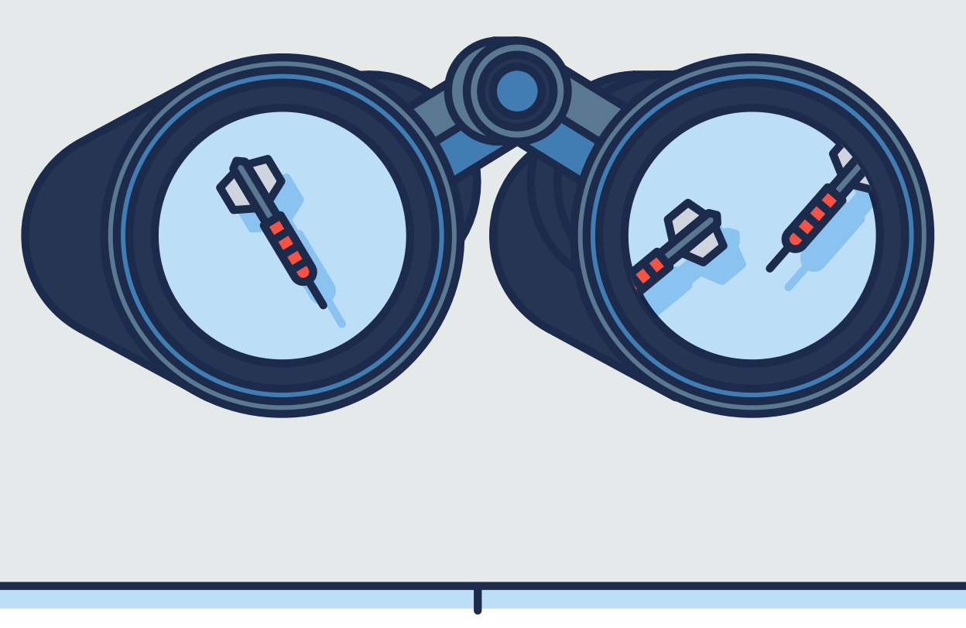


RANSOMWARE-ANGRIFF ERFOLGT

Viele Server, Desktop- und Laptop-PCs sind betroffen.

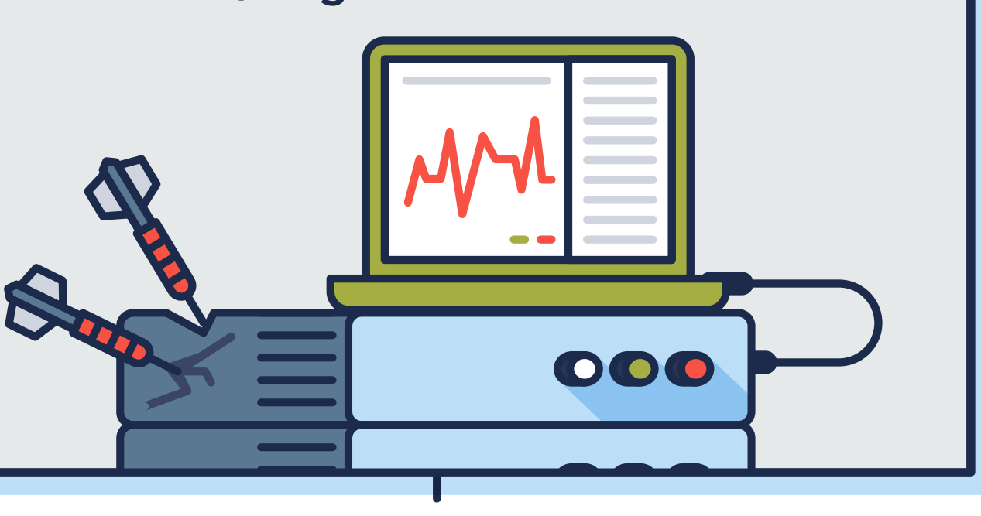
DIE IT ENTDECKT DEN ANGRIFF

Kritische Produktionsanwendungen sind lahmgelegt.



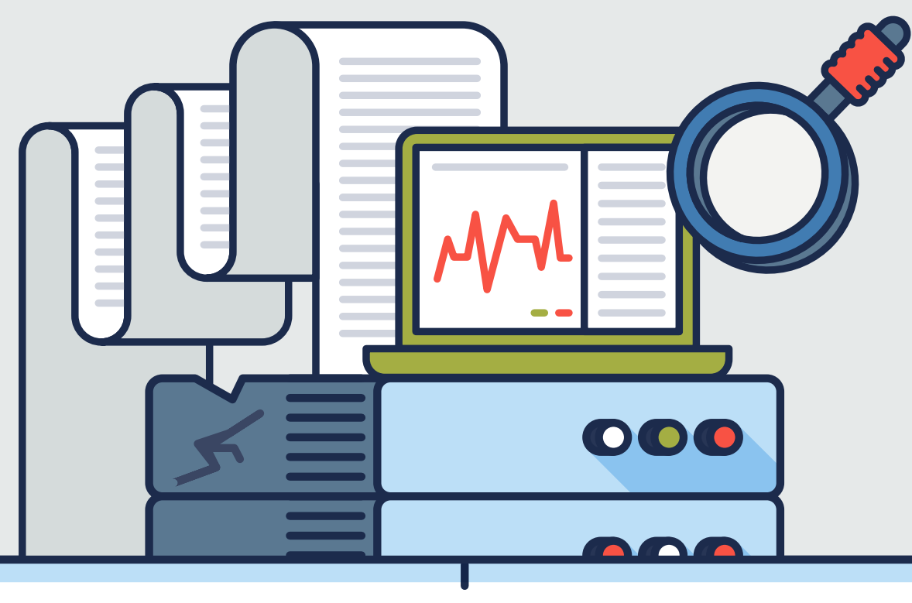
DIE IT SETZT SICH EIN, UM DEN AUSBRUCH EINZUDÄMMEN UND STARTET DEN 72-STUNDEN-COUNTDOWN ZUR BENACHRICHTIGUNG GEMÄSS DSGVO

Das Gerangel der Diagnose, welche personenbezogenen Daten verletzt wurden, beginnt. Nur kein Stress!



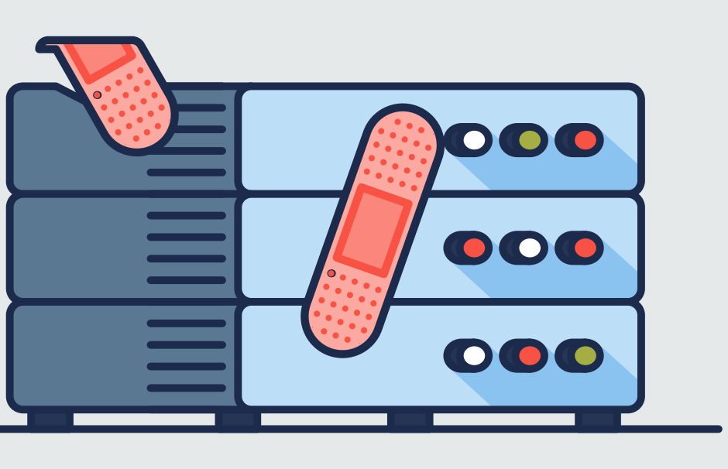
DAS UNTERNEHMEN BEGINNT MIT DER ENTSCHÄRFUNG UND ANALYSE DES ANGRIFFS

Alle Mitarbeiter – von der Rechtsabteilung bis zur Technik – arbeiten mit, um den Schaden zu stoppen.



DIE IT BEGINNT DIE WIEDERHERSTELLUNG DER VERSCHLÜSSELTEN DATEIEN AUS SICHERUNGSKOPIEN

Die IT beginnt mit der Wiederherstellung der beschädigten Dateien aus den zuletzt angelegten Sicherheitskopien.



DER DATENSCHUTZBEAUFTRAGTE BENACHRICHTIGT DIE ÖRTLICHE DSGVO-AUFSICHTSBEHÖRDE

Der Datenschutzbeauftragte informiert die örtliche Aufsichtsbehörde über die Verletzung: Art der Attacke, Anzahl der betroffenen personenbezogenen Daten, Maßnahmen zur Wiederherstellung.

DAS UNTERNEHMEN BEGINNT, KUNDEN ZU BENACHRICHTIGEN

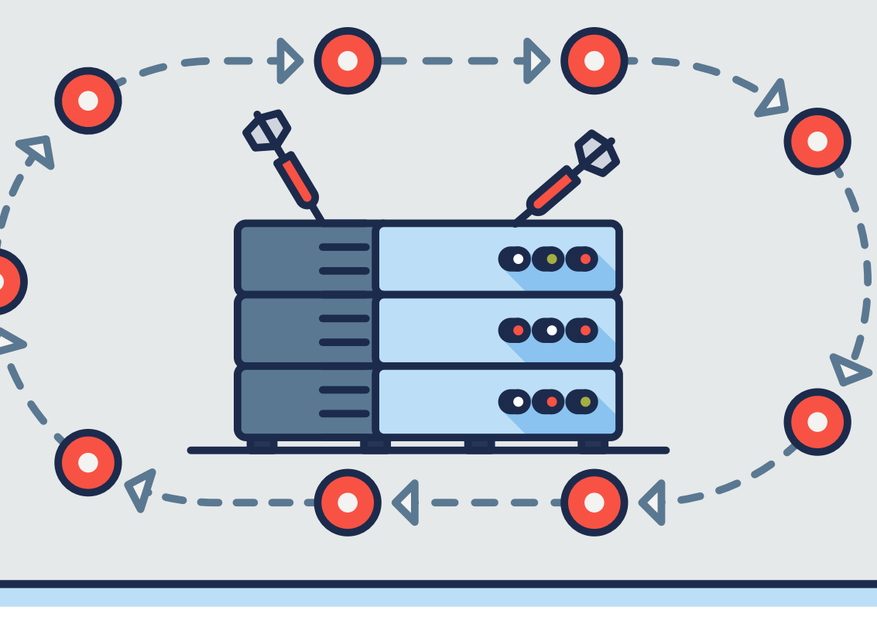
Falls es sich um eine ernsthafte Verletzung handelt, müssen alle betroffenen Datensubjekte darüber in Kenntnis gesetzt werden, was geschehen ist, an wen sie sich wenden können, was zu erwarten ist und welche Maßnahmen zur Eindämmung bereits ergriffen werden.

DAS UNTERNEHMEN BEZAHLT BUSSGELDER FÜR DEN COMPLIANCE-VERSTOSS

Jetzt müssen vielleicht die Bußgelder für Compliance-Verstöße in Höhe von 2 bis 4 % des Jahresumsatzes oder 10 bis 20 Mio. Euro (es gilt der jeweils größere Betrag) gezahlt werden.

UND NUN DAS GANZE NOCHMAL VON VORN

Ohne bessere Schutzmaßnahmen gegen Ransomware wird sich dieser Zyklus mit dem nächsten Ransomware-Angriff unweigerlich wiederholen.



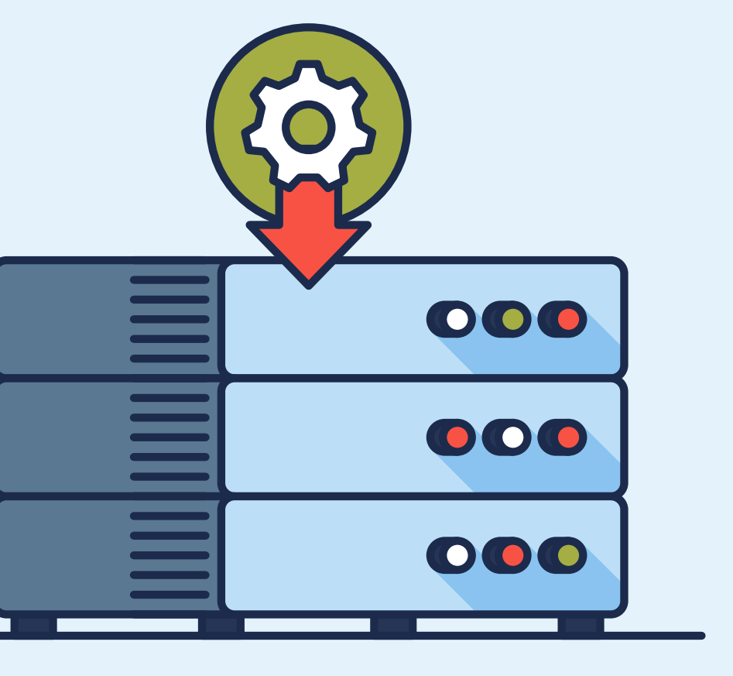
UNTERNEHMEN Y

KEINE VERLETZUNG, KEINE PROBLEME

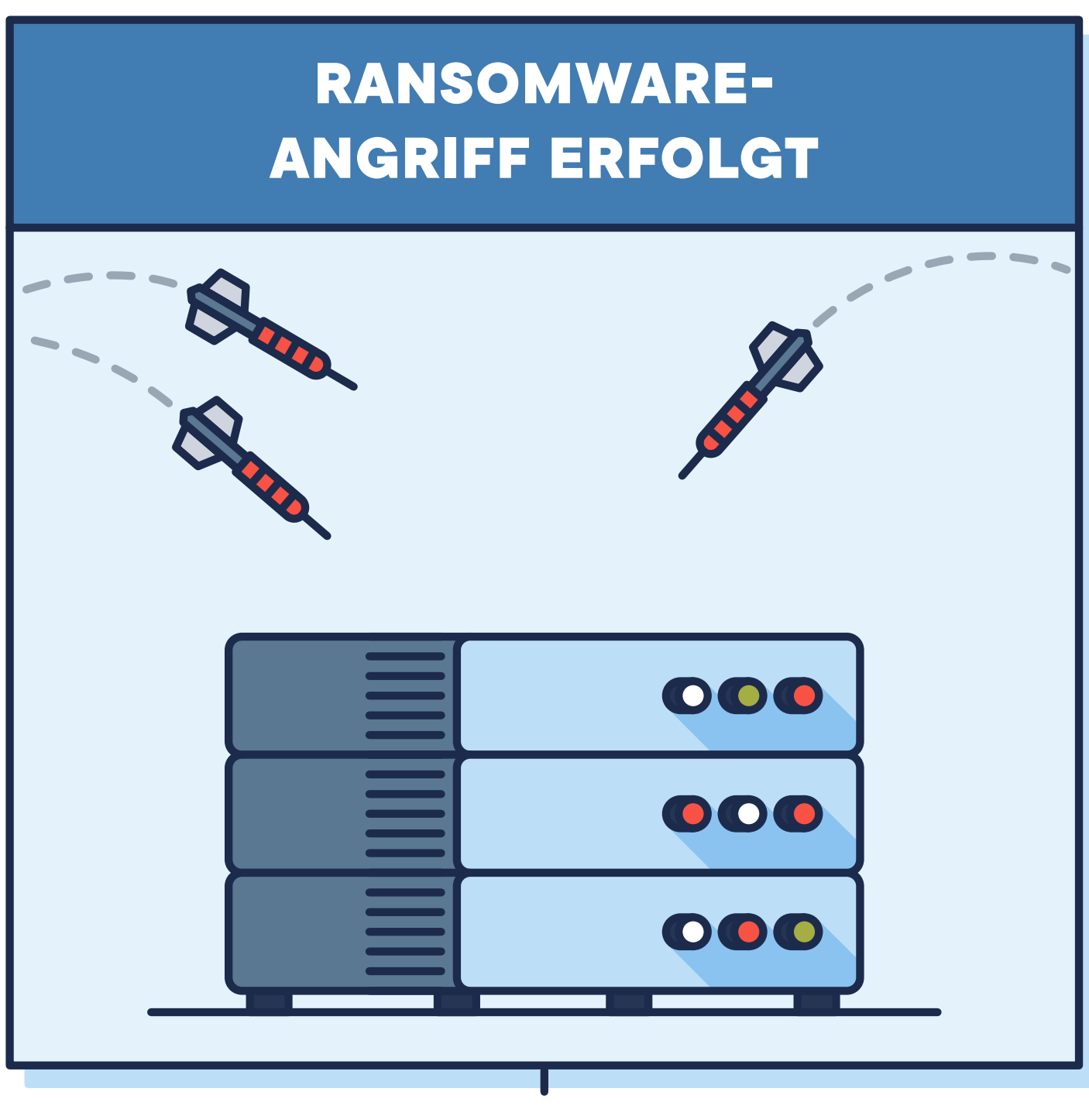
Unternehmen, die über das gesamte DSGVO-Szenario im Bilde sind, erkennen, dass Ransomware eine ernsthafte Compliance-Bedrohung darstellt, und ergreifen Abwehrmaßnahmen, bevor Verletzungen entstehen.

Schauen Sie sich diesen Verlauf an:

DAS UNTERNEHMEN INSTALLIERT ACRONIS BACKUP MIT ACTIVE PROTECTION ZUR VERMEIDUNG VON RANSOMWARE-ANGRIFFEN



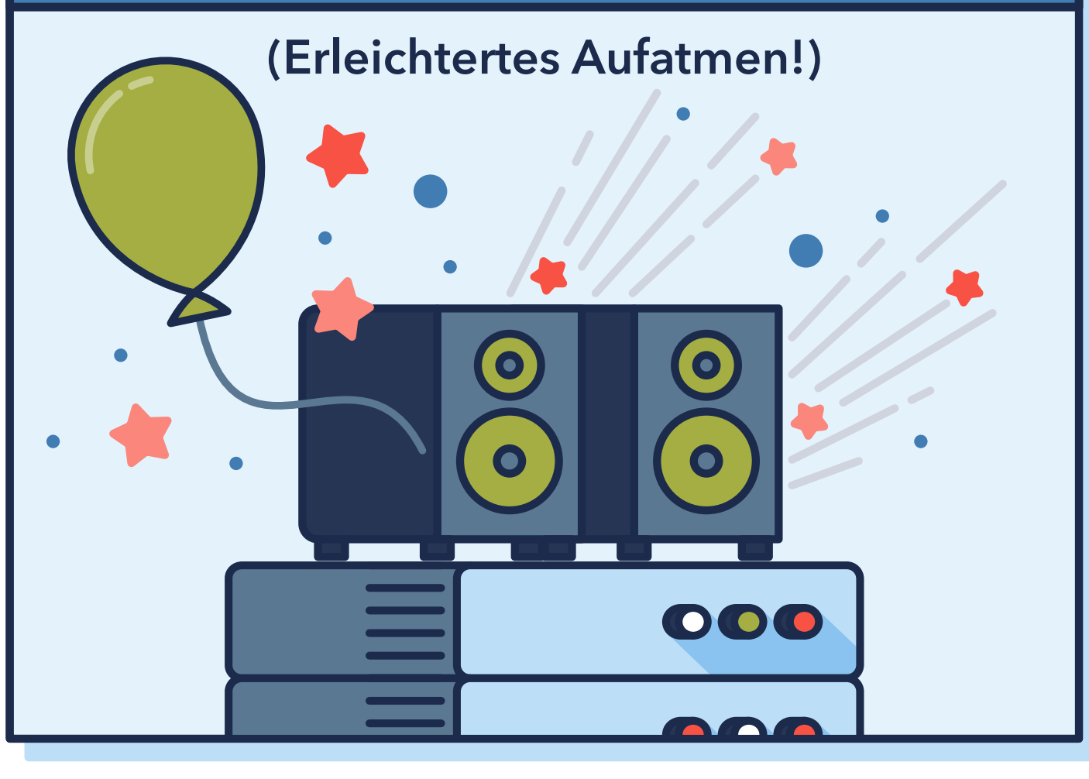
RANSOMWARE-ANGRIFF ERFOLGT



ACRONIS ACTIVE PROTECTION ENTDECKT DEN VORGANG AUTOMATISCH UND UNTERBINDET IHN

DAS UNTERNEHMEN KANN DIE BENACHRICHTIGUNG ÜBER EINE SICHERHEITSVERLETZUNG GEMÄSS DSGVO VERMEIDEN

(Erleichtertes Aufatmen!)



BLEIBEN SIE DSGVO-KONFORM MIT ACTIVE PROTECTION

Der Umgang mit den Komplexitäten des DSGVO ist eine Herausforderung, aber Sie können durch den Einsatz wirksamer Schutzmaßnahmen gegen Ransomware eine riesige Bedrohung vermeiden. Nutzen Sie Acronis Backup und Acronis Backup Cloud mit Active Protection und vermeiden Sie künftige Sorgen über die wachstumsstärkste Ursache von Sicherheitsverletzungen gemäß DSGVO.

Probieren Sie es jetzt

Von
Acronis
gesponsert