ENJOY SAFER TECHNOLOGY™

IT-SICHERHEIT FÜR KMU – EIN SURVIVAL GUIDE

Von Stephen Cobb, Senior Security Researcher bei ESET

In der von Digitalisierung geprägten heutigen Welt sind auch kleinere Unternehmen ohne den Einsatz von IT und Internet kaum mehr denkbar. Gerade auf Ebene der kleinen und mittelständischen Betriebe fehlt jedoch oftmals das Bewusstsein, dass dies auch erhebliche Risiken mit sich bringt. Einige Risiken, wie der Diebstahl physischer Objekte oder die Zerstörung von Assets durch Naturkatastrophen lassen sich durch verantwortungsbewusstes Verhalten und sinnvolle Vorsichtsmaßnahmen wirksam eindämmen. Wesentlich komplizierter ist der Umgang mit Risiken, die durch sogenannte Cyberkriminalität entstehen, also beispielsweise dem gezielten Diebstahl von Informationen oder Daten und deren Verkauf auf dem Schwarzmarkt.

Mehr als 70 % aller Datenschutzvorfälle geschehen in kleinen und mittelständischen Unternehmen. Dennoch glauben auch weiterhin viele Verantwortliche, dass ihre Firma aufgrund der geringen Größe und vermeintlich wenig wertvollen Daten für Angreifer nicht interessant wäre. Ein Trugschluss mit teils dramatischen Folgen.

Dieser Survival Guide soll Ihnen helfen, Ihr Unternehmen gegen die Folgen von Cyberkriminalität zu schützen.

Persönliche Daten, also solche, die beispielsweise für Identitätsdiebstahl verwendet werden können, sind ein besonders beliebtes Ziel von Kriminellen. Solche Daten werden selbst von kleinsten Unternehmen verarbeitet, z. B. in Kunden- oder Lieferantendatenbanken. Weiterhin interessant sind Zahlungsinformationen, z. B. Kreditkartendaten, Kontodaten, Passwörter für Onlinebanking und E-Mail-Accounts sowie Zugangsdaten zu Online-Diensten wie PayPal.

Diese Daten lassen sich lukrativ auf dem Schwarzmarkt an andere Kriminelle verkaufen, welche diese wiederum für unterschiedlichste illegale Aktivitäten einsetzen.

Folgen von Datenlecks

Auch wenn es häufig nicht im Fokus der Aufmerksamkeit steht: Unternehmen jeder Größe, die persönliche und finanzielle Daten von Nutzern verarbeiten, können im Fall des Diebstahls oder Verlusts dieser Daten für negative Folgen verantwortlich gemacht werden – beispielsweise, wenn Nutzerdaten entwendet und für betrügerische Aktivitäten genutzt werden.

Datenschutzregelungen wie die EU-DSGVO fordern zudem, dass Unternehmen Datenschutzvorfälle umgehend melden – dazu gehören auch der gestohlene Dienstlaptop oder der verloren gegangene USB-Stick mit sensiblen Informationen.

Auf die Praxis bezogen ergibt sich selbst für kleinste Unternehmen die Verpflichtung, im Unternehmen verarbeitete Daten Dritter systematisch zu schützen. Jegliche Vorsichtsmaßnahmen sollten dabei detailliert dokumentiert werden – unter anderem, um Mitarbeiter über ihre Pflichten in Sachen Datenschutz aufzuklären.

[1] IDC-Studie zu kleinen und mittelständischen Unternehmen in den USA, 2014-2018.

Doch auch große Unternehmen fordern von ihren kleineren Zulieferern mittlerweile nicht selten Nachweise darüber, dass ihre Mitarbeiter eingehend über den Schutz von Daten und seine Umsetzung geschult wurden und dass angemessene Sicherheitsvorkehrungen zur Absicherung sensibler Daten getroffen wurden. Sollte Ihr Unternehmen von einem Datenleck betroffen sein, können Sie mithilfe entsprechender Dokumentation nachweisen, dass Sie alles getan haben, um einen solchen Vorfall zu verhindern und seine negativen Folgen so gering wie möglich zu halten.

Was zu tun ist

Folgen Sie unseren Schritten von A bis F, um Ihr Unternehmen und die verarbeiteten Daten umfassend zu schützen.

- **ASSESS** – Dokumentieren Sie Ihre Assets, Risiken und Ressourcen
- **BUILD** – Stellen Sie Sicherheitsrichtlinien auf
- **CHOOSE** – Wählen Sie passende Kontrollmechanismen
- **DEPLOY** – Implementieren Sie die Kontrollmechanismen
- **EDUCATE** – Schulen Sie Mitarbeiter, Führungskräfte und Zulieferer
- **FURTHER** – Weiterführende Dokumentation, Prüfung, Tests

Sehen wir uns die einzelnen Schritte etwas genauer an:

ASSESS – Dokumentieren Sie Ihre Assets, Risiken und Ressourcen

Erstellen Sie eine Liste Ihrer IT-Infrastruktur, also alle Geräte und Services, die im Unternehmen verwendet werden. Schließlich können Sie nur das schützen, von dem Sie wissen, dass es da ist. Denken Sie auch an Mobilgeräte wie Smartphones und Tablets, mit denen Sie oder Ihre Mitarbeiter Zugriff auf Unternehmens- oder Kundendaten haben.

Man schätzt, dass etwa 60 % aller Mitarbeiter Sicherheitsvorkehrungen ihrer Mobilgeräte umgehen – 48 % deaktivieren sogar vorgegebene Sicherheitseinstellungen.

Zwei-Faktor-Authentifizierung

Vor allem für kleinere Unternehmen ist die so-genannte Zwei-Faktor-Authentifizierung (2FA) eine komfortable Lösung zur Absicherung sensibler Daten.

Es hat sich gezeigt, dass viele Datenlecks in der Vergangenheit hätten verhindert werden können, wenn Daten nicht allein durch Passwörter ge-schützt worden wären. 2FA sorgt dafür, dass Mit-arbeiter zusätzlich zu ihren normalen Login-Daten zum Beispiel ein automatisch generiertes, zufälliges Einmal-Passwort eingeben müssen, das auch nur kurze Zeit bzw. für diese Session gültig ist. Daten sind so besser vor Missbrauch geschützt, da An-greifer Passwörter nicht einfach erraten können.

Mit einer zusätzlich abgesicherten Authentifizie-rung schützen Sie Daten und Geräte vor Miss-brauch durch Dritte und sorgen zugleich dafür, dass Sie gesetzliche Anforderungen zum Datenschutz erfüllen.

Listen Sie unbedingt auch Onlinedienste, die in Ihrem Unternehmen verwendet werden, wie Salesforce, Online Banking-Webseiten sowie Cloud-Dienste (iCloud, Google Docs etc.).

Gehen Sie anschließend jeden Punkt auf der Liste durch und überlegen Sie, welche Risiken sich aus der Nutzung ergeben. Was oder wer ist jeweils die Gefahr? Eine weitere sinnvolle Frage wäre: Was könnte alles schiefgehen? Auch wenn manche Risiken wahrscheinlicher sind als andere, sollten Sie alle auflisten und Sie dann nach ihrer Eintrittswahrscheinlichkeit und der Schwere der möglichen Folgen sortieren.

Eventuell benötigen Sie hierbei Unterstützung von interner (entsprechend geschulte Mitarbeiter) oder externer Seite (Partner, Zulieferer). Deshalb sollten Sie eine weitere Liste anlegen, in welcher Sie dokumentieren, welche Ressourcen Sie in Sachen IT-Sicherheit mobilisieren können.

[2] The Cost of Insecure Mobile Devices in the Workplace, Ponemon Institute, 2014.

Als EU-basiertes Unternehmen können Sie zudem auf Unterstützung durch staatliche oder andere Organisationen zurückgreifen, beispielsweise Europol, CERT-EU, ENISA (die Europäische Agentur für Netz- und Informationssicherheit).

Nicht zuletzt müssen Sie sicherstellen, dass Ihre Mitarbeiter wissen, wie sie sich datenschutzkonform verhalten. Regelmäßige Schulungen sind unverzichtbar.

BUILD – Stellen Sie Sicherheitsrichtlinien auf

Jede noch so durchdachte Sammlung von Sicherheitsrichtlinien ist wertlos, wenn sie nicht durchgesetzt wird. Diese Durchsetzung beginnt bei Ihnen. Als Chef sind Sie in der Pflicht, deutlich zu machen, wie wichtig Ihrem Unternehmen die Vertraulichkeit und Sicherheit der verarbeiteten Daten ist. Machen Sie klar, was die Richtlinien konkret bedeuten, also zum Beispiel, dass es Unberechtigten verboten ist, auf Unternehmensdaten zuzugreifen oder dass Mitarbeiter nicht die Berechtigung haben, Sicherheitseinstellungen ihrer Mobilgeräte zu ändern.

CHOOSE – Wählen Sie passende Kontrollmechanismen

Nur mit den richtigen Kontrollmechanismen können Sie sicherstellen, dass die sorgsam ausgearbeiteten Sicherheitsrichtlinien auch umgesetzt werden. Um zum Beispiel sicherzustellen, dass kein Dritter Zugriff auf unternehmensinterne Systeme und Daten bekommt, können Sie den Zugang per Nutzername, Passwort und Zwei-Faktor-Authentifizierung beschränken (siehe Kasten).

Um zu kontrollieren, welche Programme auf Dienstrechnern installiert werden, vergeben Sie Administratorrechte nur an ausgewählte Personen (z. B. IT-Mitarbeiter). Zur Vermeidung von Datenlecks nach Diebstahl oder Verlust von Mobilgeräten können Sie Mitarbeiter anweisen, entsprechende Vorfälle noch am selben Tag zu melden – und dafür sorgen, dass die entsprechenden Geräte sofort aus der Ferne gesperrt und gespeicherte Daten gelöscht werden.

Drei grundlegende Technologien sollten Sie aber mindestens implementieren:

- eine Anti-Malware-Lösung, die verhindert, dass Schadcode auf Unternehmensrechner heruntergeladen wird,
- Verschlüsselungssoftware, die Daten für Kriminelle selbst im Fall von Diebstahl oder Verlust unbrauchbar macht – hiermit folgen Sie auch den Empfehlungen der DSGVO,
- Zwei-Faktor-Authentifizierung, die sicherstellt, dass nicht nur per Nutzername und Passwort auf Systeme und Daten zugegriffen werden kann.

DEPLOY – Implementieren Sie die Kontrollmechanismen

So banal es klingt: Bei der Implementierung Ihrer zuvor festgelegten Kontrollmechanismen ist unbedingt darauf zu achten, dass diese auch funktionieren. Haben Sie beispielsweise eine Richtlinie erlassen, dass kein Dritter Zugriff auf Unternehmens-IT haben darf, können Sie dies unter anderem über die Verwendung einer Anti-Malware-Lösung sicherstellen. Diese identifiziert schädliche Software, die Fremden Kontrolle über Mitarbeiter-PCs geben soll. Nun reicht es nicht, die Lösung nur zu installieren und zu überprüfen, ob sie eventuell Prozesse behindert. Ebenso sollten Sie für die Mitarbeiter die Schritte dokumentieren, die ergriffen werden müssen, falls die Sicherheitssoftware anschlägt.

EDUCATE – Schulen Sie Mitarbeiter, Führungskräfte und Zulieferer

Es reicht nicht, Ihren Mitarbeitern die Sicherheitsrichtlinien Ihres Unternehmens und die damit verbundenen Abläufe auf den Tisch zu legen. Sie müssen auch verstehen, warum diese Maßnahmen notwendig sind. Schulen Sie Ihre Mitarbeiter eingehend und sorgen Sie dafür, dass sie die Richtlinien verinnerlichen

– die vermutlich effektivste Maßnahme zur Steigerung der Sicherheit Ihres Unternehmens.

Wichtig ist vor allem, dass Sie gemeinsam mit Ihren Mitarbeitern daran arbeiten, das Bewusstsein für Sicherheitsfragen, z. B. aktuelle Phishing-Attacken, zu erhöhen. Erst kürzlich konnte in einer Studie gezeigt werden, dass 21 % aller Phishing-Mails an Angestellte geöffnet wurden. Immerhin 16 % öffneten die mitgeschickten Anhänge. Wird derartigem Verhalten nicht entgegengewirkt, sind Sicherheitsvorfälle kaum vermeidbar.

Dabei sollten Sie darauf achten, wirklich alle am Unternehmen Beteiligten einzubeziehen, auch leitende Angestellte, Zulieferer und Partner. Denken Sie auch daran, dass die Missachtung von Sicherheitsrichtlinien Folgen haben muss. Fehlende Konsequenz ist hier fehl am Platz.

FURTHER – Weiterführende Dokumentation, Prüfung, Tests

Die Absicherung Ihrer Unternehmens-IT ist kein einmaliges Projekt, sondern ein fortlaufender Prozess. Prüfen Sie regelmäßig, mindestens jedoch einmal im Jahr, ob die Sicherheitsmaßnahmen noch den externen und internen Gegebenheiten entsprechen. Halten Sie sich über die aktuellen Entwicklungen der Bedrohungslage auf dem Laufenden. Gute Anlaufstellen sind Sicherheits-Blogs wie WeLiveSecurity.de, KrebsOnSecurity.com oder DarkReading.com.

Dabei kann es natürlich nötig sein, Ihre Sicherheitsrichtlinien und Kontrollmechanismen immer wieder zu überarbeiten, insbesondere dann, wenn sich interne Umstände geändert haben, wie neue Lieferanten und Projekte, neue Mitarbeiter oder Abgänge. Insbesondere bei Letzterem ist Aufmerksamkeit geboten, da dafür gesorgt werden muss, dass der ehemalige Mitarbeiter keinen Zugriff auf Unternehmensressourcen mehr hat. Überlegen Sie auch, ob Sie eventuell externe Berater beauftragen wollen, um Penetrationstests und Sicherheitsaudits durchzuführen. Nur wenn Sie Ihre verwundbaren Punkte kennen, können Sie sie auch adressieren.

Es ist unwahrscheinlich, dass Cyberkriminalität in den nächsten Jahren abnehmen wird. Unternehmen sind entsprechend in der Pflicht, Daten und IT-Infrastrukturen abzusichern, um den reibungslosen Geschäftsbetrieb zu gewährleisten und die Sicherheit der verarbeiteten sensiblen Daten zu wahren.

Stephen Cobb beschäftigt sich seit mehr als 25 Jahren mit dem Schutz von Daten. Mit seiner Erfahrung unterstützt er US-amerikanische Regierungsorganisationen und einige der größten Unternehmen der Welt dabei, verarbeitete Informationen verlässlich vor Missbrauch zu schützen. Cobb war an der Gründung zweier erfolgreicher IT-Sicherheitsfirmen beteiligt, die später von börsennotierten Unternehmen aufgekauft wurden. Er verfasste zahlreiche Bücher und mehrere hundert Artikel zum Thema IT-Sicherheit. Seit 1996 ist er zertifizierter Sicherheitsberater. Cobb lebt in San Diego und ist dort Mitglied des ESET Global Research Teams.

Seit über 30 Jahren ist ESET führend in der Entwicklung von Sicherheitssoftware für Unternehmen und Endkunden auf der ganzen Welt. ESETs leistungsfähige, nutzerfreundliche Produkte sorgen dafür, dass Nutzer und Unternehmen IT sicher nutzen können. Das Portfolio reicht dabei von Endpoint- und Mobilgeräteschutz bis zu Verschlüsselungslösungen und Zwei-Faktor-Authentifizierung. Die ESET Produkte arbeiten unauffällig im Hintergrund und schützen Ihre IT-Infrastruktur rund um die Uhr, selbst vor neuesten Gefahren. Weitere Informationen finden Sie unter www.eset.de.