Computer Security Day 2023: Versteckte Kosten bei unzureichender IT-Betreuung

Vier häufige IT-Risiken und Strategien zu deren Vermeidung

(Wien, 30.11.2023) Hacking-Angriffe auf die IT-Infrastruktur von Unternehmen führen nicht nur zu Imageschäden, sondern oft auch zu erheblichen finanziellen Verlusten. Fehlende Sicherheitsupdates, oder unvorhergesehene Schadensfälle mit katastrophalen Datenverlusten ohne Backup-Strategie sind nur einige der Probleme, denen sich Unternehmen immer wieder stellen müssen. Der Ausfall von geschäftskritischen IT-Prozessen bringt Stillstand und damit erhebliche potenzielle Umsatzeinbußen mit sich. Wir wollen den heutigen Computer Security Day zum Anlass nehmen, vier häufige Risiken und Strategien zu deren Vermeidung vorzustellen.

Imageschaden und finanzielle Verluste durch Hack-Angriffe

Allein in Deutschland entstanden laut dem Wirtschaftsschutzbericht 2022 durch Cybercrime Schäden in der Höhe von rund 203 Milliarden Euro für Unternehmen. Cyberangriffe verursachen allerdings nicht nur unmittelbare finanzielle Schäden, sondern schwächen oft auch das Vertrauen in das betroffene Unternehmen und beeinträchtigen so deren Image nachhaltig. Ein markantes Beispiel hierfür ist der Angriff auf Sony Pictures im Jahr 2014. Hacker, die sich selbst die "Guardians of Peace" nannten, erbeuteten damals vertrauliche Daten, darunter persönliche Informationen über Mitarbeiter, interne E-Mails und sogar unveröffentlichte Filme und veröffentlichten diese. Dieser Vorfall zog nicht nur massive finanzielle Verluste in mehrstelliger Millionenhöhe nach sich, sondern führte auch zu einem Reputationsverlust für Sony.

Man muss allerdings nicht über den Ozean schauen, um Beispiele für Angriffe auf Schwachstellen in der IT großer Unternehmen zu finden. Im Jahr 2020 wurde A1, der größte Telekommunikationsanbieter Österreichs, Ziel eines massiven Angriffs. Der Angriff zog sich dank eingeschränkter Ressourcen während des ersten Covid-19 Lockdowns über mehrere Monate hin und kompromittierte die internen Systeme. Dieser Vorfall offenbarte nicht nur Schwachstellen in der IT-Infrastruktur von A1, sondern schadete auch dem Ruf des Unternehmens in Bezug auf Datensicherheit.

Zugriff erhalten Cyberkriminelle oft über Social Engineering-Praktiken, indem sie sich etwa als Führungskraft, Kunde oder gar IT-Betreuer ausgeben, um das Vertrauen von Mitarbeitern auszunutzen. „Die Sensibilisierung und Schulung von Mitarbeitern ist hier neben dem technischen Ausbau robuster Cybersicherheitsmaßnahmen eine wichtige Investition, um in Unternehmen eine starke Resilienz gegen derartige Bedrohungen aufzubauen“, weiß Marco Gschaider, Geschäftsführer des Wiener IT-Dienstleisters Iphos IT Service. „Oft sind es ganz einfache Dinge, wie der Check einer Absender-E-Mail-Adresse oder eines Links, bevor man vertrauensvoll auf diesen klickt, die vielen Mitarbeitern nicht bewusst sind. Aber genau diese Dinge können Hackern Tür und Tor öffnen.“

Iphos IT Service GmbH
Khekgasse 35
A-1230 Wien

+43 1 869 84 00
+43 1 869 84 00 50
office@iphos.com
iphos.com

Erste Bank, BIC: GIBAATWW
IBAN: AT602011184095568000
CEO: Ing. Christoph Wendl,
Marco Gschaider,
Handelsgericht Wien, Sitz Wien
FN 513426p,
ATU74517347

Unentdeckte Sicherheitslücken: Risiko durch effektives Patchmanagement minimieren

Unentdeckte Sicherheitslücken, sogenannte Zero Day Lücken in Software und Systemen stellen ein signifikantes Risiko für Unternehmen jeder Größe dar. Diese Schwachstellen können von Hackern ausgenutzt werden, um unbefugten Zugriff auf sensible Daten zu erlangen oder Systeme zu kompromittieren. Lässt man sich nach dem Bekanntwerden einer solchen Lücke zu viel Zeit, um verfügbare Patches einzuspielen, geht man ein hohes Risiko ein. Ein bekanntes Beispiel für die Auswirkungen solcher Schwachstellen ist der Angriff auf Equifax im Jahr 2017. Dabei wurden die persönlichen Daten von etwa 147 Millionen Menschen offengelegt. Ursache war damals eine bereits bekannte Sicherheitslücke in der Webanwendungssoftware Apache Struts, für die sogar ein Patch verfügbar war. Allerdings verabsäumte Equifax diesen auch zeitnah anzuwenden.

Ein prägnantes Beispiel für die Folgen unzureichender IT Sicherheit im DACH-Raum ereignete sich 2015 im Deutschen Bundestag. Hacker konnten über Sicherheitslücken in das Netzwerk des Bundestags eindringen und dort Daten abgreifen. Die Angreifer sollen über mehrere Wochen unentdeckt im Netzwerk operiert haben, bevor der Angriff endlich entdeckt wurde.

„Vernachlässigtes Patchmanagement ist eine Einladung an Cyberkriminelle und bringt ein erhöhtes Risiko für Angriffe mit sich. Oft sind fehlendes Problembewusstsein, ungünstige Risikoeinschätzungen oder auch Sparzwang der Grund dafür," weiß Gschaider aus Erfahrung. „Nur regelmäßige Updates können dem Ausnutzen von Sicherheitslücken vorbeugen. Bei der Wartung der IT-Infrastruktur zu sparen, weil doch ohnehin alles läuft, ist ein oft gemachter Fehler. Wir werden oft erst gerufen, wenn es leider schon zu spät ist. Proaktives Patch- und Update-Management ist das Um und Auf. Ich kann gar nicht oft genug betonen, wie wichtig regelmäßige Überprüfungen auf verfügbare Software-Updates und eine schnelle Implementierung dieser Patches sind."

Neben dem Patchmanagement sollten allerdings weitere Sicherheitsmaßnahmen zum optimalen Schutz des Netzwerks nicht vernachlässigt werden. Dazu gehören unter anderem Firewalls, Intrusion-Detection-Systeme und regelmäßige Sicherheitsaudits.

Datenverluste bei unvorhergesehenen Schadfällen: Vorsorge als Schlüssel zur Risikominimierung

„Die Wichtigkeit von Aufbau und Wartung redundanter Systeme und Backups sind ebenfalls nicht zu unterschätzen," erzählt Gschaider. „Unternehmen werden von Ransomware-Angriffen überrascht und haben keinen Zugriff auf ihre Daten und Systeme mehr. Die beste Strategie ist auch hier wieder Prävention durch Daten-Backups." Durch Ransomware sind Hacker in der Lage, Dateien zu verschlüsseln und Lösegeldzahlungen für die Freigabe zu erpressen. Ein markantes Beispiel für schwerwiegende, wenngleich zum Glück nicht dauerhafte Datenverluste ist der

Iphos IT Service GmbH
Khekgasse 35
A-1230 Wien

+43 1 869 84 00
+43 1 869 84 00 50
office@iphos.com
iphos.com

Erste Bank, BIC: GIBAATWW
IBAN: AT602011184095568000
CEO: Ing. Christoph Wendl,
Marco Gschaider,
Handelsgericht Wien, Sitz Wien
FN 513426p,
ATU74517347

Ransomware-Angriff auf das Universitätsklinikum Düsseldorf aus dem Jahr 2020. Der Angriff führte zu einem umfassenden Systemausfall. Kritische Patientendaten waren nicht zugänglich, und der Krankenhausbetrieb wurde erheblich gestört. Es war vorübergehend nicht möglich, Notfallpatienten aufzunehmen, die durch den so längeren Transport in andere Kliniken teilweise in Lebensgefahr gebracht wurden. Die Kriminellen nutzten für ihren Angriff eine Schwachstelle in einer weit verbreiteten kommerziellen Software.

„Ransomware ist nicht der einzige Grund für umfassende Datenverluste," so IT-Experte Marco Gschaider. „Brände, Diebstall oder schlicht und einfach Hardware-Versagen können ohne umfassende Backup-Strategien zum Super-GAU für ein Unternehmen werden. Wir entwickeln daher gemeinsam mit unseren Kunden umfassende Notfallpläne, damit im Fall eines Datenverlusts die schnelle Wiederherstellung von Daten und Systemen möglich ist."

Neben umfassenden Backup-Strategien, die regelmäßige und getrennt gespeicherte Backups umfassen sollten, ist auch die Konzeption eines auf alle Eventualitäten ausgerichteten Disaster-Recovery-Plans entscheidend, um im Falle eines Cyberangriffs oder technischen Ausfalls schnell - und richtig - handeln zu können.

Ausfall kritischer Geschäftsprozesse: Risikomanagement zur Minimierung von Umsatzverlusten

Der Ausfall kritischer Geschäftsprozesse ist für Unternehmen meist mit erheblichen finanziellen Verlusten behaftet. Ein solcher Ausfall kann durch eine Vielzahl von Faktoren verursacht werden, unter anderem durch technische Probleme, Cyberangriffe oder Naturkatastrophen. Ein Beispiel hierfür aus dem DACH-Raum ist der Vorfall bei der Lufthansa Anfang 2023. Ein durchtrenntes Kabel führte in Frankfurt zu massiven Flugstornierungen und -verzögerungen. Nicht gerade angenehm für die betroffenen Passagiere und für die Fluglinie mit erheblichen finanzielle Einbußen verbunden.

„Ein konkreter Business Continuity Plan kann den Ausfall geschäftskritischer IT-Prozesse zwar nicht verhindern," erläutert Gschaider. „Aber zumindest sind Unternehmen damit für den Fall des Falles gewappnet und können detailliert den optimalen Schritten zur raschen Behebung des Ausfalls kritischer Systeme folgen."

Eine starke und zuverlässige IT-Infrastruktur ist entscheidend, wenn es darum geht, Ausfälle zu vermeiden und die Geschäftskontinuität zu gewährleisten. Vorsorge ist besser als Schadensbegrenzung – eine Investition in eine robuste, qualitativ hochwertige IT-Infrastruktur schafft dieses notwendige Maß an Zuverlässigkeit. Dazu gehören auch redundante Systeme und Backup-Lösungen. Diese können im Falle des Ausfalls eines Systems raschest möglich dessen Funktionen übernehmen.

„Wo genau die potenziellen Schwachstellen in den Geschäftsprozessen liegen, das sollte durch regelmäßige Risikobewertungen identifiziert werde," so Gschaider abschließend. „Eine regelmäßige Überprüfung und Bewertung von Risiken macht es

Iphos IT Service GmbH
Khekgasse 35
A-1230 Wien

+43 1 869 84 00
+43 1 869 84 00 50
office@iphos.com
iphos.com

Erste Bank, BIC: GIBAATWW
IBAN: AT602011184095568000
CEO: Ing. Christoph Wendl,
Marco Gschaider,
Handelsgericht Wien, Sitz Wien
FN 513426p,
ATU74517347

möglich, diese auch proaktiv anzugehen. Unzureichende IT-Betreuung ist eines dieser Risiken und der Computer Security Day eine kleine Erinnerung, dieses Risiko zu beheben.“

Über Iphos IT Service GmbH

Iphos IT Service GmbH ist ein internationales Unternehmen, das Dienstleistungen in den Bereichen IT-Infrastruktur, IT-Wartung und IT-Consulting anbietet. 2019 aus der bereits 1998 in Wien gegründeten Iphos IT Solutions GmbH hervorgegangen, betreibt Iphos IT Service einen weiteren Standort in Bulgarien (Sofia). Die Dienstleistungen werden in Österreich, Deutschland, Schweiz und Bulgarien vertrieben. Ing. Christoph Wendl leitet gemeinsam mit Marco Gschaider als Chief Executive Officer (CEO) das Unternehmen, das sich mit innovativen Lösungen den aktuellen Herausforderungen der IT stellt.

Rückfragehinweis für Medien:

Marco Gschaider
Geschäftsführer, Iphos IT Service GmbH
Khekgasse35
1230 Wien
Tel.: +43 1 869 84 00
E-Mail: marketing@iphos.com
https://www.iphos.com

Iphos IT Service GmbH
Khekgasse 35
A-1230 Wien

+43 1 869 84 00
+43 1 869 84 00 50
office@iphos.com
iphos.com

Erste Bank, BIC: GIBAATWW
IBAN: AT602011184095568000
CEO: Ing. Christoph Wendl,
Marco Gschaider,
Handelsgericht Wien, Sitz Wien
FN 513426p,
ATU74517347