IT-Sicherheitslücken in der Pflege mit **Pentesting** erkennen

von Matthias Niedung (Berater für IT-Sicherheit und Datenschutz bei Althammer & Kill)

Plötzlich geht nichts mehr – ein Unternehmen aus dem Diakonieumfeld mit mehr als 2.000 Mitarbeitenden muss im Sommer 2022 feststellen, dass es Opfer einer BlackCat-Erpressungssoftware-Attacke geworden ist. Hunderte von Laptops und Computern sind plötzlich verschlüsselt, Mitarbeitende können nicht mehr auf Dateien, IT-Systeme und Arbeitsmittel zugreifen, ein Weiterarbeiten ist kaum mehr möglich. Die Lösegeldforderung lässt nicht lange auf sich warten. Solche Angriffe sind der Worst Case für Pflege- und Gesundheitseinrichtungen und bei Weitem keine Einzelfälle mehr.

Das Bundesamt für Sicherheit in der Informationstechnik meldete zuletzt bis zu 553.000 neue Schadprogramm-Varianten pro Tag! Dem „Allianz Risk Barometer 2022" zufolge sehen 44 % der befragten Verantwortlichen Angriffe auf ihre IT-Systeme als das größte Geschäftsrisiko. Penetrationstests sind ein wirksames Mittel, um Cyberangriffe einzudämmen.

Penetrationstests sind professionelle Überprüfungen der eigenen IT-Systeme, um Sicherheitslücken zu identifizieren und zu schließen. Dabei verüben „legale Hacker*innen" Angriffe auf die IT-Landschaft und identifizieren Einfallstore für einen Cyberangriff. Welche Systeme und Prozesse genau getestet werden sollen, legt die beauftragende Organisation selbst fest: Sollen alle IT-Systeme überprüft werden, um einen umfassenden Überblick über den Status Quo zu erhalten, oder ist ein Check eines neu implementierten Systems gewünscht?

Foto: Althammer & Kill

Für wen sind Pentestings relevant?

Die vom BlackCat-Angriff betroffene Organisation wäre ein klassischer Kunde für ein Pentesting gewesen. Sie verfügt über mehrere Standorte, eine weitverzweigte IT-Landschaft, stationär und mobil agierende Mitarbeitende und eine große Menge sensibler Daten. Wobei Letzteres auf fast alle in

der Gesundheits- und Pflegebranche tätigen Unternehmen zutrifft. Cyberangriffe beschränken sich dabei keineswegs ausschließlich auf „große“ Organisationen. Auch kleine und mittelständische Einrichtungen sind betroffen.

Wie läuft ein Penetrationstesting ab?

Ein Penetrationstesting verläuft in der Regel in vier Phasen. Zunächst verschaffen sich die Penetrationstester*innen einen Überblick über die Organisation. Eine sogenannte Open Source Intelligence (OSINT) soll dabei E-Mail-Adressen, versteckte Verzeichnisse oder verborgene Systeme ausfindig machen. So gehen auch Cyberkriminelle vor. Dabei handelt es sich heute um gut vernetzte Organisationen und ausgebildete Teams, die ihr Know-how und ihre Infrastruktur auch weiteren Angreifenden zur Verfügung stellen und anschließend am Lösegeld beteiligt werden.

Das Pentesting-Team nutzt die gewonnenen Informationen, um Angriffe auf die identifizierten Lücken zu planen. So können kompromittierte E-Mail-Adressen für sogenannte Phishing-Kampagnen genutzt werden, bei denen den Mitarbeitenden vorgegaukelt wird, eine E-Mail von einem ihnen bekannten Absender zu bekommen und sie verleitet, auf einen Link zu klicken, der Schadsoftware auf den Rechner lädt. Aber auch versteckte IT-Systeme, sogenannte Schatten-IT, die ohne das Wissen von IT-Administrator*innen von Mitarbeitenden installiert wurde, eignet sich sehr gut für Angriffe.

Bei den gefundenen Wegen ins System spricht man von Angriffsvektoren, die je nach Art des Systems und Services stark variieren können. Pentester*innen genauso wie Hacker*innen können dabei auf automatisierte Tools zurückgreifen, die ihnen helfen, den Ist-Zustand der IT-Landschaft genau zu überprüfen. Sind Lücken identifiziert, starten tatsächliche Angreifer*innen in einer zweiten Phase erste Interaktionen und Tests mit der Infrastruktur.

Diese Tests können sich über einen langen Zeitraum hinziehen, bevor die tatsächliche Attacke erfolgt. Die Penetrations-Tester*innen werden in dieser Phase erstmals eine ausführliche Rücksprache mit den Auftraggebenden durchführen, aus denen erste Maßnahmen für die IT-Sicherheit abgeleitet werden können.

Der geplante Angriff beginnt

Sind die Lücken identifiziert und die Tests abgeschlossen, erfolgt der Angriff. D. h., die Pentester*innen machen sich

Weiter auf Seite 44

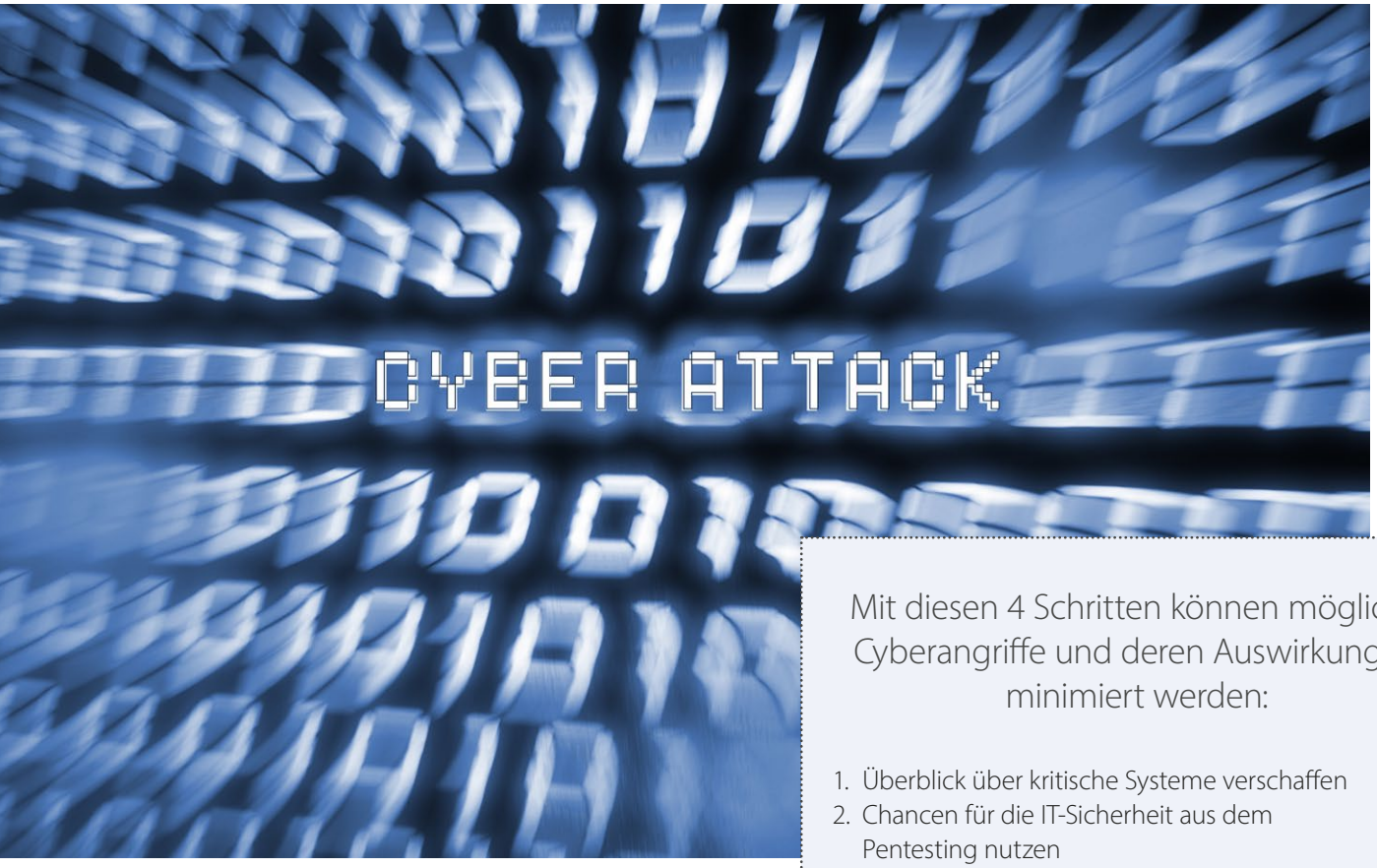

Foto: MargJohnsonVA– envato

Wichtig: Nur wenn Mitarbeitende geschult und für Angriffsvektoren sensibilisiert sind, minimiert sich das generelle Risiko von Cyberattacken.

Mit diesen 4 Schritten können mögliche Cyberangriffe und deren Auswirkungen minimiert werden:

1. Überblick über kritische Systeme verschaffen
2. Chancen für die IT-Sicherheit aus dem Pentesting nutzen
3. Systeme und Prozesse optimieren und fit machen für eine digitale Zukunft
4. Ressourcen für stetige Cyber-Sicherheit einplanen

auf den Weg, von außen in die Systeme einzudringen. Welche Angriffsvektoren zum Einsatz kommen, hängt von der vorherigen Priorisierung ab. Mit dem zuvor gesammelten Wissen über Software, Prozesse, Systeme, Updates und Gepflogenheiten in der Organisation wird ein realistisches Angriffsszenario erstellt. Über kleine Lücken sind professionelle Hacker in der Lage, weitere Türen aufzumachen und immer weiter in Systeme vorzudringen. Wenn es den Penetrations-Tester*innen gelingt, Schwachstellen ausfindig zu machen, diese mit sogenannten Exploits (kleine Schadsoftware-Programme) zu erweitern und in die Systeme einzusteigen, haben sie ihr Ziel erreicht. Die Auftraggebenden können aus diesem geplanten Angriff eine tatsächliche Attacke vorwegnehmen und die Lücken schließen. Das ist das Ziel eines jeden Penetrationstests.

Analyse der Ergebnisse und Learnings

Der Weg in die Systeme wird von den Pentester*innen genau dokumentiert und analysiert. So sind die Verantwortlichen einer Organisation in der Lage, die Risiken zu erfassen und entsprechende IT-Sicherheitsstrategien zu erarbeiten (siehe Infokasten).

Neben der regelmäßigen Pflege der IT-Systeme, muss auch der zweite Weg, den Cyberkriminelle nutzen, um in ein System einzudringen, im Fokus bleiben: die Mitarbeitenden. Nur wenn sie geschult und für Angriffsvektoren sensibilisiert sind, minimiert sich das Risiko von Cyberattacken insgesamt.

Das Risiko von Cyberkriminalität ist bei den Vorständen und Geschäftsführenden angekommen, es fehlt oft lediglich die Erkenntnis, dass ein dauerhaft hoher Schutz der eigenen Systeme nur mit der Einplanung von Mitarbeitendenressourcen und Budgets erreicht werden kann. Es braucht klare Verantwortlichkeiten und Sicherheitskonzepte sowie Maßnahmen, um die eigenen Daten und die Systeme sinnvoll zu schützen.

Das oben genannte Unternehmen hatte Glück im Unglück. Nicht alle Systeme waren gleichermaßen betroffen und aufgrund funktionierender Backups ist es gelungen, Daten wiederherzustellen, während die infizierten Systeme isoliert werden konnten. Es wurde kein Lösegeld gezahlt, aber der Schaden war da – große Teile der Organisation waren über einen längeren Zeitraum nicht arbeitsfähig. Die IT-Struktur musste neu aufgebaut, neue Hardware angeschafft werden. Die IT-Sicherheit wird seither einen hohen Stellenwert haben.