MARKTBERICHT

Was kostet wie viel?

Jetzt frisch aus der Region

Rotkraut:
konventionell
1,20 Euro / kg
Bio 2,40 Euro / kg

Möhren:
konventionell
1,20 Euro / kg
Bio 1,70 Euro / kg

Grünkohl:
konventionell
3,20 Euro / kg
Bio 4,90 Euro / kg

Porree:
konventionell
3,00 Euro / kg
Bio 3,90 / kg

Über die aktuellen Preise informiert Sie der Biohof Gaus-Staubitz aus Wittelsberg.

ES STAND IN DER **OP**

Vor 10 Jahren

Berlin. Besuch beim Kinderarzt wird Pflicht
Der Schutz der Kinderrechte wird nicht ins Grundgesetz aufgenommen, Bund und Länder wollen aber mehr für den Kinderschutz tun. Unter anderem soll eine weitere Vorsorgeuntersuchung im dritten Lebensjahr hinzukommen.

Marburg. Einige Kneipen im Kreis stehen vor Schließung
„Das Rauchverbot versetzt einigen Kneipen den Todesstoß", sagt die Betreiberin des „Molly Malone's". Einige Kneipen im Kreis haben bereits geschlossen, viele andere beklagen Umsatzeinbußen. Unterstützung erhalten die Gastwirte von der FDP.

Vor 25 Jahren

Bonn. 500 000 Lichter gegen Ausländerhaß
Knapp eine halbe Million Menschen demonstrierten von Nord bis Süd wieder mit Lichterketten gegen Fremdenhaß und Ausländerfeindlichkeit in Deutschland.

Marburg. Streit: Wer sind die wahren Grünen?
Gegen seinen Parteiausschluß legt Hermann Rottmann, der für die Grüne und Alternative Linke (GAL) kandidiert, Widerspruch ein. Er selbst finde es zwar auch „pervers, mit einem originären grünen Programm gegen die offiziellen Grünen zu kandidieren", sehe sich aber zu diesem Schritt durch innerparteiliche Auseinandersetzungen gezwungen.

Vor 50 Jahren

Brüssel. Londons zweiter Anlauf zur EWG scheiterte
Es bestehen keine Aussichten, daß angesichts der starren französischen Haltung in absehbarer Zeit direkte Verhandlungen über einen Beitritt Großbritanniens, Irlands, Dänemarks und Norwegens zum Gemeinsamen Markt stattfinden.

Marburg. Studentenparlament lehnt 15,4 v.H. ab
Den Vorschlag des Großen Senats der Philipps-Universität, die Studentenschaft mit 15,4 Prozent im satzungsgebenden Senat zu beteiligen, lehnte das Studentenparlament mit 23 zu 14 Stimmen ab.

Je smarter, desto angreifbarer

OP-Serie „Aber Sicher" · Folge 2: Cyberkriminalität · So können sich Nutzer vor Netz-Angriffen schützen

Der Virus kommt per Post. In E-Mail-Anhängen und Links stecken die Gefahren. Eine gesunde Skepsis kann vor eigenen größeren Schäden bewahren.

von Katja Peters

Hacker brauchen oftmals nicht mehr als ein paar persönliche Daten, um ihre Opfer auszuspionieren.
Archivfoto: Uli Deck

Marburg. Würmer, Viren, Trojaner, DDoS-Attacken (von englisch: Distributed Denial of Service, „verbreitete Verweigerung des Dienstes") – wer im Internet unterwegs ist, sollte sich gegen genau solche Angriffe schützen. Zu denken, dass man als Privatnutzer verschont bleibt, ist leichtsinnig. Das findet jedenfalls Dirk Hintermeier, der beim Polizeipräsidium Mittelhessen als Präventionsbeamter über Cyberkriminalität, also über die Gefahren aus dem Internet, aufklärt.

19 735 Fälle registrierte er im Jahr 2016 hessenweit. „Aber die Dunkelziffer ist viel, viel höher", weiß er und erklärt: „Viele Menschen schämen sich, dass sie einem Betrüger auf den Leim gegangen sind oder erstatten bei niedrigen Beträgen keine Anzeige." Denn in sein Ressort fallen auch Betrügereien in Sachen Internethandel. Ein Beispiel: In kleineren Online-Shops oder auf Auktionsplattformen soll oft per Vorkasse bezahlt werden. Unvorsichtige Käufer überweisen das Geld, erhalten aber nie ihre Ware, gerade jetzt im Weihnachtsgeschäft. „Das ist oft so, wenn Luxusgüter wie hochwertige Telefone oder Fernseher zu einem Bruchteil des normalen Preises angeboten werden", sagt der Polizeibeamte.

Vor allem in den Sozialen Medien gibt es immer wieder diese Angebote, um Kaufinteressenten auf externe Webseiten zu locken. „Genau das wollen die Kriminellen", betont auch Heinz-Joachim Eifert. Der IT-Spezialist aus Marburg warnt davor, blauäugig im Internet zu surfen und überall mal drauf zu klicken oder ein „Gefällt mir" zu hinterlassen. „Was heute wie ein seriöser Online-Shop aussieht, kann in zwei Wochen schon die Seite eines Kinderpornorings sein", erklärt er und fügt hinzu: „Wenn dann ermittelt wird, kann es schon mal sein, dass auf einmal die Polizei vor der Tür steht und den Computer einkassiert, weil der Verdacht besteht, dass der unbedachte Internetnutzer womöglich einen Kinderpornoring unterstützt. Da fallen viele aus allen Wolken." Daher warnt auch er davor, sich zu vertrauensselig im Internet zu bewegen.

Firewall und Virenscanner sollten daher auch immer installiert und aktiv sein. Ebenso ist ein aktualisiertes Betriebssystem unerlässlich, um technische Geräte zu schützen. Denn für beide Experten steht fest, dass die meisten Bedrohungen über E-Mails versendet werden. In Anhängen oder per Verlinkungen, die im Text mitgeschickt werden, befinden sich die Fallen. Ein Klick und der Nutzer landet wieder auf dubiosen Internetseiten. Dieser Klick kann bewirken, dass sich Schadprogramme auf dem eigenen Rechner selbst installieren – oft vom Nutzer erst einmal unbemerkt. Die Software kann Passwörter auslesen und dann großen Schaden anrichten. Daher raten beide Experten generell zu einem sensiblen Umgang mit Passwörtern. Niemals sollte überall das gleiche verwendet werden. Standardbestandteile sind Groß- und Kleinschreibung, Zahlen und Sonderzeichen. „Je länger, desto besser. Und es sollte öfter mal geändert werden", so Dirk Hintermeier. Auch die Nutzung von gleichen Passwörtern auf der Arbeit sowie im Privaten sehen beide kritisch.

Wurde die Schadsoftware erfolgreich installiert, kann der eigene Rechner auch quasi zum Helfer für ein sogenanntes Botnet werden. Das ist eine Gruppe automatisierter Schadprogramme, sogenannter Bots. Die Bots (von englisch: robot „Roboter") laufen auf vernetzten Rechnern, deren Netzwerkanbindung sowie lokale Ressourcen und Daten ihnen, ohne Einverständnis des Eigentümers, zur Verfügung stehen. Der infizierte Rechner agiert durch Schadsoftware gesteuert, versendet beispielsweise permanent Anfragen an Server großer Unternehmen oder Behörden. Der private Rechner ist so ganz schnell Teil einer sogenannten DDoS-Attacke. 2012 wurde auf diese Art die Webseite der Stadt Frankfurt am Main, im Rahmen der Blockupy-Proteste, lahm gelegt. Zweck solcher Angriffe sind meist Erpressung, Schädigung eines Konkurrenten oder Spionage beziehungsweise Sabotage des Zielsystems.

Aber es geht auch kleiner: Erpressung mit dem eigenen Rechner. Ist so ein Schadprogramm durch Unwissenheit des Nutzers installiert, macht es das System langsamer, verschickt beispielsweise Viren an Freunde aus dem Adressbuch oder verschlüsselt die Festplatte des Rechners. Dann bekommt der Eigentümer eine Meldung, aus der hervor geht, dass er seine Daten nur durch Zahlung einer Summe X zurück bekommt. „Viele machen das dann einfach, weil sie ihre privaten Daten, Fotos oder Programme nicht verlieren wollen", so Dirk Hintermeier, der warnt: „Auf keinen Fall bezahlen, sonst würde man das kriminelle Geschäftsmodell der Täter ja noch fördern."

Regelmäßig Daten sichern – Kettenbriefe löschen

Bekanntestes Beispiel dafür ist der „Bundes-Trojaner", durch den Kriminelle Millionenschäden verursacht haben. „Daran sieht man, welche Macht diese Täter haben", so der Polizeibeamte, der noch einmal betont: „Vorsicht bei Links, die per E-Mail gesendet werden. Wenn der Absender unbekannt ist und dem Empfänger suggeriert wird, dass er über diesen Link weitere Informationen bekommt, dann ist Vorsicht geboten." Überhaupt sollten Internet-Nutzer immer eine gesunde Skepsis walten lassen. „Bevor man irgendwo draufklickt oder einfach auf OK drückt, lieber drei Mal durchatmen und hinterfragen", rät der Präventionsbeamte und fügt hinzu: „Eine regelmäßige Datensicherung auf einer externen Festplatte kann im Falle eines Datenverlustes sehr hilfreich sein.

Heinz-Joachim Eifert sieht das genauso und warnt eindringlich davor Dateien mit den Endungen „zip" oder „exe", die per E-Mail versendet wurden, zu öffnen oder gar eine Installation zu starten. Das seien mitunter Ausführdateien – „und die installieren immer etwas. Im schlimmsten Fall eben Schadsoftware", so der Experte. Im Zweifelsfall sollte der Nutzer die Anhänge vorher durch den Virenscanner analysieren lassen. Das funktioniert aber eben nur bei Anhängen, die Links in E-Mails checkt der Virenscanner nicht. Die Täter nutzen zum verbreiten meist fingierte Layoutmails namhafter Firmen, wie beispielsweise DHL. „Wer nichts bestellt hat, bekommt auch keine Meldung. Also sofort löschen", sagt Dirk Hintermeier.

Gleiches gilt auch für die vielen neuen „Smart-Geräte". Der Backofen, der von unterwegs angestellt werden kann, das Heizungsthermostat, das per Handy reguliert wird oder die Überwachungskamera, die im Urlaub oder von der Arbeit aus neu ausgerichtet werden kann. „Jedes Teil, das mit dem Internet kommuniziert, öffnet auch Türen für Täter", erklärt Heinz-Joachim Eifert und fügt hinzu: „Je smarter und vernetzter ich bin, desto angreifbarer werde ich auch."

Angreifen sollen auch Kettenbriefe, die per Sozialen Medien und Nachrichtendiensten von Handy zu Handy verschickt werden. Aber nicht das mobile Gerät an sich ist hier das Ziel, sondern die Psyche des Nutzers. Er soll verunsichert werden, wird aufgefordert, den Brief an viele Freunde weiterzuleiten, damit ihm nichts Schlimmes zustößt. Dirk Hintermeier warnt dennoch: „Manche Briefe haben auch Links oder enthalten Aufforderungen auf einer Website Zugangs- oder Kontodaten einzugeben. Dem sollte man auf keinen Fall nachkommen. Am besten: gleich löschen!" Kettenbriefe oder sogenannten Hoax (von englisch: hoax, altengl. hocus: Scherz, Falschmeldung) sind immer gleich aufgebaut:

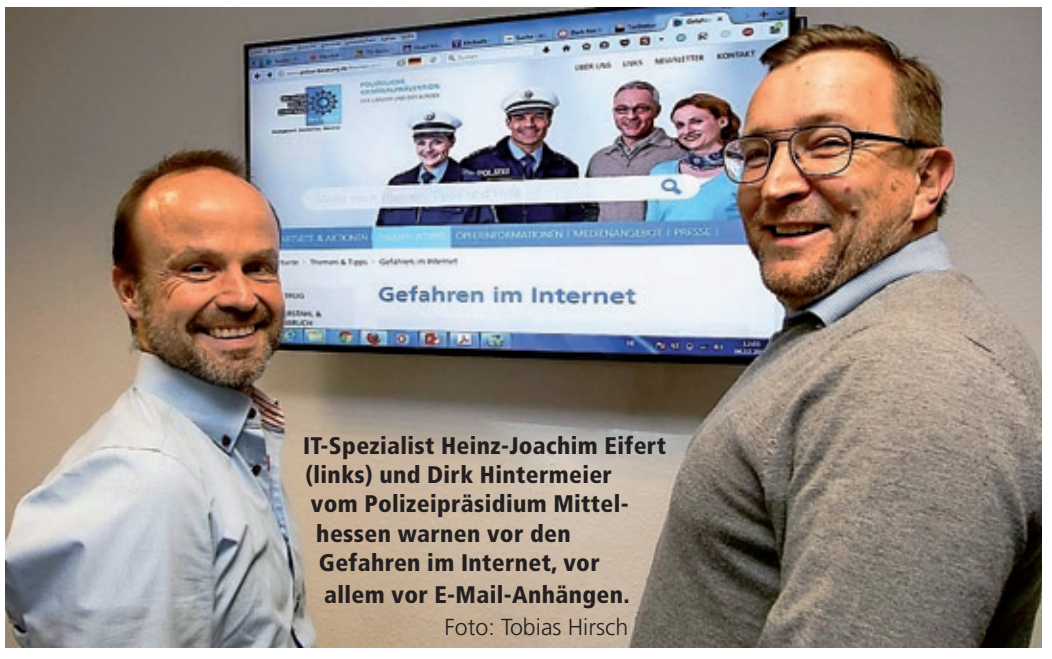
- Der Adressat wird aufgefordert, die „Warnung" an möglichst viele Menschen weiterzuleiten.
- Der Betreff enthält oft den Begriff „Virus Warnung" oder sinnverwandtes. Die Wirkung des Virus wird sehr drastisch dargestellt und beinhaltet Dinge, die ein Computer-Virus gar nicht kann (z.B. Hardware beschädigen).
- Häufig wird als Quelle eine namhafte Firma oder Organisation genannt, um die Glaubwürdigkeit zu verbessern. Bei diesen Firmen finden sich jedoch keine Hinweise auf eine solche Warnung.
- Oft finden sich Aktualitätsangaben wie „gestern" oder „am Freitag", die keinen Bezug zu einem bestimmten Datum haben können. Wenn ein Kettenbrief schon ein paar Tage, Wochen oder Monate unterwegs ist – wann war dann „gestern"?!

Das Internet ist voll von hilfreichen Informationen, aber es tummeln sich eben auch jede Menge Kriminelle. Vorsicht ist geboten, Grund zur Panik gibt es dennoch nicht.

Informationen zu diesen Themen finden Sie im Internet unter www.polizei-beratung.de

Checkliste Cyberkriminalität

1. Betriebssystem immer aktuell halten
2. Firewall installieren und aktualisieren
3. Virenscanner installieren und aktualisieren
4. Passwörter regelmäßig ändern und unterschiedliche Passwörter nutzen
5. Kettenbriefe löschen
6. regelmäßige Datensicherung
7. .zip und .exe-Anhänge in E-Mails nie öffnen
8. Links in E-Mails von unbekannten Absendern, die auf unbekannte Webseiten weiterleiten, nicht anklicken
9. Kaufangebote im Internet mit unrealen Preisen für Luxuswaren oder gar Schenkangebote ignorieren
10. Vorkassaufforderungen bei unbekannten Händlern nicht nachkommen



IT-Spezialist Heinz-Joachim Eifert (links) und Dirk Hintermeier vom Polizeipräsidium Mittelhessen warnen vor den Gefahren im Internet, vor allem vor E-Mail-Anhängen.
Foto: Tobias Hirsch